DIGITAL WAR

The One Cybersecurity Strategy You Need To Implement NOW To Secure Your Business

Yigal Behar

Digital War

The *One* Cybersecurity Strategy You Need to Implement *Now* to Secure Your Business

Yigal Behar

August 2017

Digital War—The *One* Cybersecurity Strategy You Need to Implement *Now* to Secure Your Business

Printed in the United States of America.

First published: August 2017

ISBN: 9798873857340

About the Author

Yigal Behar is a seasoned Cyber Security professional with over 25 years under his belt, Mr. Behar parlayed his experience consulting for high-profile entities like the Israeli Prime Minster Office and other governmental agencies, banks such as Bank Hapoalim into his entrepreneurial pursuits. In 2003, he launched 2Secure Corp, his second venture, and has since dedicated himself to its growth and success. He believes in personalized client engagement, leveraging his expertise and business development skills to deliver custom solutions.

To share his cybersecurity expertise and guide small and medium-sized business owners and managers, Mr. Behar launched "The Cybersecurity Insider" podcast. Tune in on YouTube for valuable insights and guidance. Don't miss out on valuable tips - subscribe today!

Who Should Read This Book

This book was written for the small-business owner and C-level folks who are looking to improve their knowledge in the realm of cybersecurity. Digital transformation is a *top* priority to survive the digital age; information is more important than money. Another point is that, personally, I'm so upset and angry that people are not really doing anything and are too busy covering their asses (sorry for my language). You see, I read and handle cases of network-breach stories on a *daily* basis now, and everyone is talking about stricter regulations and data sharing, yet the basics are left behind, giving any hacker easy access to our most valuable assets.

Don't become an easy prey.

I hope you will find this book helpful, and you are welcome to share your thoughts by e-mail: Cyber@2Secure.biz. I will be more than happy to learn from *you*!

Contents

Chapter 1: Genesis

I decided to write this book to help small-business owners understand how cyber threats can affect their business, in addition to other issues like cash flow, sales, customer retention, and other aspects of small-business management and operations. As a security professional and IT person who, for the past twenty-five years, has worked with owners and C-level persons, I find it interesting; why don't they get it?

This is so vital to their success, so why are they *not* making some decisions?

After all, owners and C-level people are smart, have a vision in mind, and are truly motivated and committed to their business success, just as I relate to my own business—there is a disconnect here.

A Short Story

One Friday, I got a call from Peter. He was referred to us by one of our business partners. That manager told me, "We have a problem; I think we have breached."

My first question was, "How do you know?"

He replied, “We saw some transactions that we do not recognize.”

After arriving at the scene and reviewing some evidence, we told management, “Yes, you were breached, and here is what you need to do *right now*!” The cost was $100,000.

We gave them a list of actions and an estimate of $100,000. They were in shock; this is a lot of money, and so on. Well, I said, you know you can be fined for millions of dollars and possibly go to jail! Then I had the same discussion with the CFO, and he provided a third option that I could not forget: “You have given us two options, and a third would be ‘shut down the business.’”

That answer left me with an open jaw. What did I miss here?

A few days ago, I learned that the owner has sold his business…

Is selling your business can be considered a business shutdown?

Chapter 2: Digital versus Physical Security

I think most businesspeople don't understand the digital age especially well: computers, software, and cloud technology, not to mention other changes such as the Internet of things (IoT), big data, artificial intelligence, and virtual reality (check out the bonus chapter)—all will change our lives and change how we do business from day to day.

Looking back, before e-mails, we used faxes. When was the last time that you used a fax?

We can learn a lot from physical security. Look at your own home. How do you protect it from unwanted visitors? What measures do you use?

Looking back, my service for three years in the Israeli Navy taught me some lessons that I would like to share with you. We did four activities: (1) constant drills, (2) using intelligence before any mission, (3) constant learning from past events, and (4) opening our eyes and ears for the unusual.

One day we had an incident with the Jordanian navy; we observed a drifting tourist, and at the same time, we noticed a Jordanian coast-guard ship going toward that drifter. After a few minutes, we were in close proximity to each other, and indeed, we were already prepared behind our

guns, ready to go. At that moment, we could spot a huge difference between them and us; we were ready, but they were not! Guns were covered and not loaded with bolts! It would take minutes to get ready! There was no time here!

The moral of the story here: be prepared!

Chapter 3: What Do I Need?

That's a good question; let's look first at how you should be protecting your home, and this will help you understand what to have when it comes to your digital world.

When I ask businesspeople to "please list all measures you can think of protecting your home," the most common answers will include fences, locks, and an alarm system.

Defend	Discover	Remediate
Fences	Alarm system	Police
Locks	Motion detection	Dogs
Doors	Cameras	Guns
Windows	Monitoring	Insurance
	Crime watch	Guard

Table 1. The "DDR" Model

At this point, I ask, "What is the most critical column here?" Most people will say, "Defend is the most critical."

This is the one mistake that 80 percent of businesses make when securing their data: choosing the defend column.

There are a few problems when selecting the defend column; the emphasis here is more about the protection layers and not about the ability to discover and remediate an incident.

In a recent study conducted by the Ponemon Institute LLC, the mean time to detect a breach is two hundred days! From this, we can deduce that organizations cannot detect an intruder quickly enough and lock down their networks. In other words, they put all of their eggs in one basket, on the defense layer, with very little or no discovery and remediation—hence, fences and locks.

This also explains the daily news, day and night, reporting network breaches. If you don't have visibility, how can you react to these incidents?

This point brings us to the next part: how long it takes to remediate a network breach. It depends on many factors.

Detection and Remediation

In general, systems generate records of actions and transactions every second, for many purposes. This can include information about errors or developing problems on various system components that require attention sooner rather than later and often are not being watched for a long time or only whenever a problem comes up, and then it's too late.

You need to have a system and processes in place that will collect all of that data to one place for what we call an "aggregator" and that later on will drive some correlation and analytics by looking for patterns in these types of events. Once you have that in place, it will change very important aspects of any given business.

- Notice a problem and take an action.
- Improve customer satisfaction.
- Improve efficiency and service uptime.
- Improve resource utilization—hence, expenses.
- Improve resources' effectiveness.

The next part is related to the remediation: How quick and effective is the repair? In this case, you are more dependent on the experience and knowledge of your team or your outsourced IT.

In case of a breach, are they competent in cybersecurity and do they understand security and do it for living? Or do they do everything through VoIP, backups, cloud, and virtualization?

I meet many IT people from small to big companies. They all say, "We have it covered," and you probably take this at face value. I like to think of them as a general doctor; they know some things, but they are *not* specialists. If you have a heart problem, you go to someone who knows the heart better than the general doctor does.

As I’m writing this book in August 2017, it’s very tough to find someone who has the experience and the “know-how” in addition to his or her cost, and this will change as technology changes along with businesses’ needs.

Putting It All Together

Let's put together what we have discussed so far and summarize it into two questions that will help you understand this better.

1. How soon can you detect an intruder? The sooner the better because this will affect recovery costs, reputation damage, and regulatory fines.
2. How soon can you recover? This goes hand in hand with the previous question. The longer it takes, the higher the damage.

These two questions will have a great impact on businesses' operations. While these are great questions, some of the owners would come back and ask another great question: "Well, I'm a Small Business Owner. Why would some hacker-cracker be interested in my little baby? After all, I don't have anything of value for them." I know; I hear this question often. So let's look at some research data according to a Verizon Data Breach Investigation report.

Breaches by Organization Size		
Organizations Size (Employees)	Number of Breaches	Percentage of Total
1 to 10	42	4.9%
11 to 100	570	66.7%
101 to 1,000	48	5.6%
1,001 to 10,000	27	3.2%
10,001 to 100,000	23	2.7%
Over 100,000	10	1.2%
Unknown	135	15.8%
Total	855	100.0%

Table 2. *Breaches by organization size*

As table 2 illustrates, out of 855 reported breaches, 612, or just over 71 percent, occurred to companies that had between one and one hundred employees.

There are five reasons why this is happening to SMB companies:

1. The emphasis is on the defense layers.
2. They don't have the expertise.
3. They don't have enough workers to handle incidents.
4. They don't have the tools to detect incidents.
5. Finally, they can't remediate an incident.

Once they have a great target like an SMB that was already hacked the first time, they will come again because they know this one is already vulnerable.

Now, let's talk about the value. I'll break it into five values.

Hacker Value 1*:* If a hacker can control fifty or more computers as an infrastructure conducting more hacking (and they do) activities, targeting other SMBs like yours, now they can achieve much larger attacks with the ability to conceal their origin.

Hacker Value 2**:** You have employees' data—SSNs for payroll, customers' information (can be credit-card or contact information)—that can be used to drive more attacks such as identity theft.

Hacker Value 3: Other third parties that you do business with or your processes can be collected as well.

Hacker Value 4: Making money by encrypting your files and asking for a ransom. Current prices can be $500–$17,000, and this is likely to increase.

Hacker Value 5: They can use one or more values above and combine an attack to include data gathering and then encrypt the data and ask for money in return of data.

Let's look at a recent research conducted by the Ponemon Institute in June 2016; this research was based on 598 individuals in companies with a headcount from less than one hundred to one thousand. The results: 50 percent suffered a cyberattack/data breach in the past twelve months! Only 14 percent of the companies represented in this study rate their ability to mitigate cyber risks, vulnerabilities, and attacks as highly effective.

No business is too small to evade a cyberattack or data breach.

The National Cyber Security Alliance reports that one in five small businesses has been a victim of cybercrime in the last year—and that number is growing rapidly as more businesses utilize cloud computing and mobile devices and store more information online. You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity.

Because of all of this, it's critical that you protect your business from these top nine ways that hackers get into your systems.

1. **They take advantage of poorly trained employees.** The number-one vulnerability for business networks is the employees using them. It's extremely common for an employee to infect an entire network by opening and clicking on a phishing e-mail (that's an e-mail cleverly designed

to look like a legitimate e-mail from a website, vendor, clients, coworkers, or people you trust). If employees don't know how to spot infected e-mails or online scams, they could compromise your entire network.

2. **They exploit device usage outside company business.** You must maintain an acceptable use policy that outlines how employees are permitted to use company-owned PCs, devices, software, Internet access, and e-mail. I strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and unified threat management (UTM). Having this type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data.

   If that employee is checking unregulated, personal e-mail on his or her own laptop and it infects that laptop, it can be a gateway for a hacker to enter *your* network. If that employee leaves, are you allowed to erase company data from his or her phone? If his or her phone is lost or stolen, are you permitted to remotely wipe the device, which would delete all of that employee's photos, videos, texts, and so on, to ensure *your* clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit-card information, financial information, and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

3. **They take advantage of *weak* password policies.** Passwords should be at least eight characters and contain lowercase and uppercase letters, symbols, and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised easily. Again, this can be *enforced* by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

4. **They attack networks that are not properly patched with the latest security updates.** New and old vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office. Therefore, it's critical you patch and update

your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

5. **They attack networks with no backups or simple single-location backups.** Simply having a solid, reliable backup can foil some of the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, natural disasters, fire, water damage, hardware failures, and a host of other data-erasing disasters. Again, your backups should be *automated* and monitored; the worst time to test your backup is when you desperately need it to work!

6. **They exploit networks with employee-installed software.** One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games, or other "innocent"-looking apps. This can largely be prevented with security controls and employee

training and monitoring.

7. **They attack your devices when you're off the office network.** It's common for hackers to set up fake clones of public Wi-Fi access points to try to get you to connect to *their* Wi-Fi over the legitimate, safe, public one being made available to you. Before connecting, check with an employee of the store or location to verify the name of the Wi-Fi it is providing. Next, *never* access financial, medical, or other sensitive data while on public Wi-Fi. Also, don't shop online and enter your credit-card information unless you're absolutely certain the connection point you're on is safe and secure.

8. **They use phishing e-mails to fool you into thinking that you're visiting a legitimate website.** A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular website or to click and download a virus.

   Often these e-mails look 100 percent legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, and so on. That's what makes these so dangerous—they *look* exactly like a legitimate e-mail.

9. **They use social engineering and pretend to be you.** This is a basic twenty-first-century tactic. Hackers pretend to be you to reset your passwords. In 2009, social engineers posed as Coca Cola's CEO, persuading an exec to open an e-mail with software that infiltrated the network. In another scenario, hackers pretended to be a popular online blogger and got Apple to reset the author's iCloud password.

Unfortunately, smaller organizations may not have the budget and in-house expertise to harden their systems and networks against potential threats.

Moreover, the introduction of cloud applications and mobile devices is creating more security risks that will eventually stretch these companies' resources.

Note: Cybersecurity is *not* a one-time activity; it's a life-cycle activity with one measurement in mind. Are we improving from where we are now to the next twelve months?

At this point, we can all agree that something has to be done; the question is then how far do we need to go to feel comfortable with your ability to discover and respond to cyber threats?

It depends on many factors: assets' locations, asset types, security controls that are currently in place, processes, and other planned customer-facing services will predict how much you should invest to enable an effective cybersecurity program.

The Three Pillars of a Successful Incident Response Plan

The truth is that a security breach in your business is not so much about losing data or assets as it is about losing customers and customer confidence. You can always recover from anything less than a catastrophic loss of data, because with a good backup system in place, your business will be able to revert to yesterday's status at worst.

But when you've lost a significant number of customers, that's something that hits you right where it hurts: on your bottom line.

Even worse, if there's a general loss of confidence in your company's ability to protect data assets, that kind of news can spread like a California forest fire, and you may find customers rushing for the exits. That's why your business should seriously consider a suitable program tailored to your needs, which matches expert planning with guaranteed capacity to facilitate the optimal breach response.

The Breach Response

Because you simply can't survive a poor breach response with your customers, it makes good sense to reserve the capacity necessary to launch an effective breach response within the shortest possible time frame. Having all the people and other resources dedicated to this single objective and having them available at the most crucial moment can make all the difference between a successful response and one that ends up costing you customers and revenue. Here's what an incident response brings to the table.

Cost savings: Organizations implementing an incident response have the potential of realizing a 30 percent cost reduction on services in the event of a data breach. This can amount to a very significant dollar amount, and it's something you don't want to lose sight of amid the chaos of a breach.

Capacity to scale: When disaster strikes, your business will have the people and the resources standing by—people dedicated to providing the fastest and most effective response, all at a moment's notice. Should the size of the problem be more significant in nature, then resources are scaled up accordingly to match the threat.

Expert preparation: To prepare your business for the most effective response to any data breach, incident-response consultants can assess your company's needs and clearly

define the optimal plan that adequately meets the threat. This plan is then tested out to identify potential hang-ups and to ensure smooth operation when the actual event occurs.

When security breaches occur in your business, you can't afford to have your customers learn about what happened through the media because it conveys the appearance that you are completely unaware and unprepared for the situation.

Incident Response Plan

In order to launch a successful breach response plan, your organization needs to have the speed and the capacity to do so by having the right resources. This involves collaboration between your internal team of experts and incident response consultants, working together with all the resources necessary to manage and overcome the problem. Here are the fine points of what a specialized incident response program should look like.

Guaranteed collaboration: Your organization should count on external incident response experts who can collaborate quickly with your internal team to implement the customer-facing response plan that was previously developed and tested. If circumstances warrant it, adjustments can be made to the plan to increase its effectiveness, but in any case, at minimum, it should include notification, support, and identity-protection capabilities.

Response capacity: Expert resources should be mobilized that have been dedicated to your potential incidents at the agreed-upon scale.

Expert guidance should be available to advise you to the best of their knowledge and experience, based on best practices that have been developed from experience.

Readiness testing: Even if your company never experiences a data breach, on-site and off-site training can help prepare your team with periodical training sessions. Teams of experts should participate with you in detailed response drills in order to ensure readiness for the actual event. Simulations are used to test the effectiveness of procedures and of specific plan components while acquiring technical skills.

Have a plan: If your company has a plan, it will reduce your costs before and after a network breach. Team training will reduce discovery and treatment times.

The Three Pillars

To avoid that kind of embarrassment and that kind of public-relations nightmare with your customers, you need to take steps that are critical for success in managing any kind of data breach.

First, draft a response plan so that you have a road map for how to proceed and are not left clueless when the event actually occurs.

Second, make sure you have legal counsel in place to manage any kind of legal fallout associated with the event.

Last, make sure that your employees are trained adequately about security measures, which can likely help to prevent any kind of data breaches. For instance, accessing company data on smartphones and clicking on suspicious e-mail attachments or links.

In the event of some kind of breach occurring despite all this training, be sure your employees are ready to react in whatever capacity is appropriate to their role within the company.

When everyone does his or her part to maintain security, the chance of a successful breach is less likely to happen.

Chapter 4: Why Do We Have These Issues?

You probably have asked this in the past; the simple answer is human errors. What do I mean? Humans—or should I say software and hardware engineers—are creating the products and services we are using; these are created with a certain amount of knowledge, experience, and set of assumptions and all keep changing constantly as technology advances. If you have a good cybersecurity program, it will eliminate some of the above. For instance, software bugs are made by poor design or bad assumptions of how normal users will use a piece of software, not taking into account the possibility that a hacker will try to use it in many different ways.

A reasonable cybersecurity program should enable your company to shore up these holes with some compensating controls.

Is it going to be better? Unfortunately, the answer is no. In the old days, some twenty years ago, things were simpler; we used faxes. We are now sitting on the genesis of other technologies or business enhancements like the Internet of things (IoT—see the bonus chapter) that will transform businesses even more but with more security threats than before. I have to mention the mobile devices as we use them more for our daily routines, and it's clear to me that

these devices will soon take your PC off your desk! Are you getting ready?

Things will get more complicated because information or digital assets will spread everywhere. The old school of a company's perimeter that is protected by a firewall has moved to the cloud and from cloud to your smartphone. Cloud technology is a threat to your company because the security is managed by a third party that you don't control.

False Sense of Security

I had to write this section because I hear many business owners try to object to my messages about security and why they don't need to do anything or get concerned because:

My IT guy told me we are covered.

Your IT guy is like a family doctor. He knows your network, users, and applications, so the assumption is he must know his stuff. Yes, he makes things work but not necessarily secure.

When it comes to protecting your company, you need to know for certain—*without any lingering doubts*—that you are doing everything you can to avoid being an easy target for cybercriminals.

As I mentioned earlier in chapter 3, when you have a problem with your heart, you go to ask a heart specialist.

We have a firewall and antivirus. So we must be good, right?

No, a firewall is placed as your "gatekeeper," controlling what can enter or leave your network. This approach used to be effective ten to twenty years ago; nowadays, a hacker won't try to knock down a big "door" that is heavily guarded. Instead, he or she will look for an easy entry using a social engineering attack or just by sending an e-mail and waiting for some employee to click.

We have antivirus and we keep it up-to-date. So we must be good, right?

This solution has three flaws:

1. It protects from past malicious software as it uses a signature to detect a malware or a threat.
2. It takes time until you get an update, and then it's too late; you are infected.
3. It takes time until antivirus companies develop the "vaccine" for a specific case, and you have eighty thousand strains (versions) developed every *day*.

Therefore, your antivirus cannot detect new threats and protect you from future threats as they are being pushed into computers.

Chapter 5: Compliance

I know some of the readers may need to comply with some laws related to cybersecurity, the most known being the Payment Card Industry Data Security Standard (PCI DSS). You are probably thinking, “Hey, I got certified so I must be secured.” You may have checked a box, but you are far, very far, from being at the point where you can assume that.

Compliance is just some bureaucracy tricks that not necessarily help protecting data; in fact, stricter regulations are not helping to manage risk or can at least show a downward trend in the amount of network breaches. My gut feeling is telling me that this is the opposite.

If you think more about this, stricter regulations increase companies’ expenses in order to stay in compliance and do only the bare minimum required. Otherwise, they face huge fines and possibly going to jail!

The basic root cause has not been solved at all. Instead, we should be looking at threats and how to defend, discover, and remediate them, but we are too busy with papers and reports.

Now don’t get me wrong; you need it, but when you are losing the objectives, you see the trees but not the forest.

Many companies get this certification, and later on they are breached time after time with great revenue loss and C-levels lose their positions; yet no one is getting it.

So let's take a few examples of past network breaches.

Table 3. The top 20 most commonly used LinkedIn account passwords, according to LeakedSource

Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652
8	sunshine	39,118
9	qwerty	37,538
10	654321	33,854
11	000000	32,490
12	password1	30,981
13	abc123	30,398
14	charlie	28,049
15	linked	25,334
16	maggie	23,892
17	michael	23,075
18	666666	22,888
19	princess	22,122
20	123123	21,826

LinkedIn—May 17, 2016: A 2012 data breach came back to haunt LinkedIn when 117 million e-mails and password combinations stolen by hackers four years prior popped up online. At the time the breach occurred, members who had been affected were told to reset their passwords. That information then became publicly available in May 2016. LinkedIn acted quickly to invalidate passwords of all LinkedIn accounts that were created prior to the 2012 breach and had not undergone a reset since the breach. It is not clear who stole the information or published it online, but LinkedIn is actively working with law enforcement officials.

Wendy's—May 11, 2016: In January 2016, Wendy's began investigating a potential data breach after receiving reports of unusual activity involving payment cards at some of its restaurant locations. The details of that investigation became public in May as the fast-food chain revealed that less than 5 percent of its restaurants were affected. The company believes that malware infiltrated one particular point-of-sale system at fewer than three hundred of approximately fifty-five hundred franchised North America Wendy's restaurants, starting in the fall of 2015.

Security reporter Brian Krebs said many bank and credit unions "have been grumbling about the extent and duration of the breach" and that it seems some breached Wendy's locations were still leaking customer card data as late as the end of March 2016 into early April.

June 16, 2016, update: In June 2016, Wendy's announced that its data breach was worse than it originally thought. The company did not provide much additional information—only that "additional malicious cyber activity has recently been discovered in some franchise-operated restaurants." It said that it disabled the newly discovered malware but that "the number of franchise restaurants impacted by these cybersecurity attacks is now expected to be considerably higher than the 300 restaurants already implicated." Wendy's is continuing to work with security experts and federal law enforcement who are investigating the breach.

Wendy's is already the subject of multiple class action lawsuits filed on behalf of affected cardholders and the financial institutions that issued payment cards to them.

Hollywood Presbyterian Medical Center, which is owned by CHA Medical Center of South Korea, paid forty bitcoins, a virtual currency, or $17,000, to restore normal operations and disclosed the attack publicly.

That hack was first noticed February 5, 2016, and operations didn't fully recover until ten days later.

Some companies must follow the HIPAA, Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other health-care providers.

As you can read, it cost a lot of money to resume operations and often risked people's lives as well.

Do you think it's serious? I do!

Chapter 6: Ten Things You Need to Know before Securing Your Data Assets

The types and patterns of data breaches that have dominated network intrusions over the past couple of years have not recently undergone any drastic changes in methodology or approach. This represents great news for network-security personnel because it means that known intrusions can be studied and analyzed, and networks can be made secure against those particular intrusion types.

It does not mean, however, that there is nothing new happening in the world of cybercrime, nor does it mean that security officers can relax under the impression that existing measures are sufficient to safeguard vital data assets. On the contrary, greater vigilance than ever before is now required because the number of attacks is ever increasing, and any component newly added to your network can conceivably be vulnerable to attack.

With all this in mind, here are the ten most current general categories of security attack that require constant vigilance on your part. Paying close attention to these intrusion types just may prevent a data catastrophe at your company.

Denial of Service Attacks

How it works: These are attacks intended to overwhelm and compromise the performance of a network or system.

Denial of service (DoS) attacks are intended to compromise or disable the availability of networks, and they are characterized by overwhelming attacks on networks or applications, which result in either severe degradation or a complete interruption of service.

The sophistication of these attacks has increased dramatically in the last couple of years, and they are now including temporal lensing. This process sends packets along various paths with the intention of simultaneous arrival at a targeted destination for overwhelming it completely.

Typically, DoS attacks are either very large in terms of magnitude, that is, packets per second, or have long duration—both can be very effective at degrading or disabling your network.

What to do: Some of the best preventive measures you can adopt against denial of service attacks are closing down all ports on your network that are unused, blocking bad traffic through your IDS/IPS, using firewalls to filter unwanted traffic, and having an effective emergency response plan ready in case all else fails.

Crime Ware

How it works: These are opportunistic crimes involving some type of malware for the financial gain of the attacker.

The main culprits in this collection of data breaches are ransomware, spyware, keyloggers, and backdoor data exporters. Of these, ransomware is the biggest problem, which is not surprising since it has been proven extremely effective for cybercriminals, in terms of realizing quick profits paid by companies anxious for the release of data assets. Since few businesses can survive for long without access to critical data, extortion demands are often met rather than pursuing more time-consuming solutions.

What to do: The types of malware in this category are generally successful because they exploit system vulnerabilities, either on the operating system itself or in resident applications. Your best bet for avoiding these kinds of intrusions is to keep your system patched with current security controls and to make sure all your application patches are also up-to-date.

Physical Theft and Loss

How it works: These incidents involve either misplacement or outright theft of company information resources.

This category represents a surprisingly common breach of data security, since the loss of a company laptop or other mobile device can quickly be exploited if it should fall into the wrong hands. The vast majority of cases falling into this

category are actually lost laptops rather than stolen ones, although both situations provide the same opportunities to cybercriminals.

Without a doubt, any data contained on the laptop is at risk because the only control preventing access is a password, and any hacker worth his or her salt won't be stymied long by passwords. Also included in this category are individual documents containing company data or information that enables access to company assets.

What to do: The best thing you can do for situations that fall into this category is to implement a company policy of full disk encryption on all mobile devices and to develop an attitude that recognizes the value and criticality of important documents.

Insider Misuse

How it works: Employees maliciously or without authorization use company resources.

This can be one of the most dangerous of all intrusion patterns because it is based on the premise that someone on the inside is assisting a criminal partner conducting the attack or is in fact conducting the attack himself or herself from inside the network. The scary thing about this scenario is that no matter how carefully devised a security scheme is, it is rendered completely ineffective by someone who has knowledge of how to breach it internally or how to disable it at will for an attack.

Anyone who has network privileges pretty much has a free pass to carry out a cyberattack on the company network. This kind of assault is very often the most difficult to detect because it can be so well hidden by the perpetrator. Unless an investigator gets just plain lucky, this kind of attack can go unnoticed literally for months or years. Even worse, such attacks are almost impossible to stop, other than to ensure that employees having network access privileges never become disgruntled employees.

What to do: Preventing dissatisfaction among employees can go a long way toward eliminating attitudes that might lead to insider abuse of privileges. However, this isn't really the most reliable means of managing insider breaches. For that, only close and regular monitoring can ensure that employees don't provide the opening for intrusions.

Point-of-Sale Intrusions

How it works: These are remote attacks against retail outlets where credit and debit cards are swiped for payment of goods, with POS terminals and controllers being the chief targets.

Point-of-sale setups provide fruitful targets for cybercriminals because they often involve payment-card data, which are solid gold for cyber thieves. The reason point-of-sale attacks are so easy to orchestrate by criminals is that POS servers are visible to the entire Internet. POS has traditionally made use of a default login, and by using these vulnerabilities, malware can easily be installed to

capture payment-card data right at the moment of processing.

Since the first waves of POS attacks several years ago, some security measures have upped the ante by featuring increased credentialing to prevent the installation of malware. However, cyber attackers have countered this measure by making concerted efforts to steal the necessary credentials prior to conducting a planned POS attack.

What to do: Since single-authentication schemes are the single greatest weakness of POS setups, the best way to prevent them is with a secondary security method. Something like a hardware token or a full-blown mobile app can secure your POS servers against breaches.

Web Application Attacks

How it works: Incidents in which a web application is the focus of an attack, either exploiting code weaknesses or circumventing authentication.

Company websites are more important to businesses than ever, funneling traffic inward to generate sales and to promote company branding across the Internet. Websites have grown much more sophisticated and much more interactive, and this increased level of complexity can be seen as increased vulnerability as well, since there are lots more components requiring protection.

The company website is literally a gateway to underlying business logic and databases containing crucial information

about the company and its customers, so it's easy to understand that web applications have become prime targets for cybercriminals. The yield from such attacks can be enormous—and catastrophic for the company.

What to do: complex passwords are not enough to secure your site against intrusions from cyber attackers. With so many company assets at stake, it's worth your while to invest in penetration test excerise and validate all vulnerabilties and fix them before hackers will discover them for you…

Cyber Espionage

How it works: Unauthorized access is gained to networks from state-affiliated entities.

This group is characterized by external threat actors that manage to infiltrate targeted networks for finding sensitive company data and perhaps trade secrets, which might be used for criminal advantage. External threat actors are generally state-sponsored groupings and organized cybercrime groups, and once they've pilfered valuable trade secrets or other company data, it's just a short step before this information reaches the open market and returns a windfall to the perpetrators.

Most external threat actors start out with simple exploitation of company networks, and this means that close attention should be paid to areas you might not think of as being especially vulnerable. For instance, protecting against e-mail-based attacks is very important, and it

should include spam protection, block lists, and phishing detection.

What to do: Securing endpoints can be done by conscientiously managing browser and plug-in updates, keeping antivirus software current, and even installing a sophisticated endpoint threat detection and response system. Additional network protection should include two-factor authentication, segmentation of the network, and blockage of C2C communications.

Last but not least, there should always be internal monitoring of accounts and devices, daily logging of system activity, and comprehensive network monitoring.

Payment-Card Skimmers

How it works: A skimming device is illegally implanted on assets reading magnetic data from payment cards.

There's probably no cybercrime easier to pull off than payment-card skimming, and since it happens also to be one of the most profitable, it's not hard to see why this remains a very popular category of cybercrime. Nowadays, the vast majority of these crimes are related to ATMs, with a few also occurring at gas pumps.

Payment-card skimmers are generally constructed with tremendous precision by their profit-minded makers and are nearly impossible to identify with the naked eye. This makes the only reliable method of detection some kind of

sophisticated fraud algorithms or common point-of-purchase (CPP) mechanisms.

What to do: Many ATMs are built these days with a tamper-resistant design, and you should be using these units to prevent card skimming. Installing video cameras out of the reach of criminals will help to prevent installation of a skimmer, and stickers over terminal doors can be another good deterrent.

Miscellaneous Errors

How it works: Unintentional actions on the part of employees compromise the security of a network or system information.

Human errors account for a significant number of data breaches, even though employees might constantly be reminded of the importance of precision and caution when it comes to working with company data and networks. One of the most common unintentional errors in this grouping is accidental publication of critical information to an unintended audience (for instance, the whole Internet), where it can be viewed and exploited.

Something as simple as mistyping a firewall rule can allow unintended file server access to a very large audience, rather than the intended narrower grouping. Also in this category are errors with the disposal of sensitive documents. When care is not taken with such critical information, it can easily fall into the wrong hands instead of the shredder where it should have gone.

While it might seem trite to say, all employees in your company should learn from mistakes that have happened in the past and that employees at other companies have committed, some of which have been described above.

What to do: It's worth documenting all such errors that happen at your company and reminding employees in the future that such trivial mistakes really can have huge consequences. This will help to create an environment of security awareness throughout the company and help prevent avoidable human error.

Human Target Attacks

How it works: An e-mail or other socially engineered message is sent to a specific user with the intention of tricking him or her into opening a malicious attachment.

This is kind of a catchall grouping that mostly includes phishing attacks, but these are different from the garden-variety phishing attacks in that they attempt to induce humans into making judgment errors.

Most often, the scenario runs something like this: An e-mail from an important manager or CEO directs an employee to transfer funds to a specific location for an apparently legitimate reason and urges that the action be carried out promptly. This ruse may be included as part of a larger communication, but the whole point of it is to target a human individual into making a security error, allowing the sender to profit enormously.

Since what's targeted in this kind of attack is human judgment, the kind of controls that might be implemented is limited to helping employees avoid actions involving bad judgment. This means encouraging employees to question anything that seems out of the ordinary in a communication, especially something involving data or financial assets.

What to do: When employees feel comfortable about questioning things out of the ordinary, these kinds of attacks can be minimized. Conversely, if such independent thinking is discouraged, it becomes more likely that such attacks will find employees more willing to blindly carry out instructions given in bogus communications.

About the Demographics of Attacks

It doesn't really matter where you are—cybercriminals will find you, regardless of your country, your industry, or your network type. It's fair to say that the most frequently targeted industries are those associated with financial information, for obvious reasons, but any kind of data related to individuals can be put to use by criminal minds bent on gaining some kind of advantage for themselves.

It would be a grave mistake to think that your company is immune from attack simply because it is not a banking institution or does not maintain information about credit cards and savings accounts. Any data involving people's identities can and will be used by cybercriminals, so unless you stay ever alert to the dangers, your company might

easily become the newest statistic in the fight against network intrusions.

Chapter 7: Cloud Security

If you've been undecided about the move to cloud-based computing, you aren't alone, since only about 37 percent of all companies are currently adapted for cloud computing. However, a recent report issued by Emergent Research and Intuit Inc. projects that by the year 2020, approximately 80 percent of all US businesses will have fully embraced cloud computing and will conduct their businesses in that mode.

Without you realizing it, your company may already be using cloud-based applications in various business units within your organization. For instance, if your company uses Dropbox as a means of exchanging documents or sharing them, you've already been using cloud-based applications.

Not surprisingly, these and a myriad of other web-based programs are enormously popular because of some of the inherent advantages that cloud-based computing imparts to them, namely tremendous flexibility, built-in automation, economy of scale, and universality of access via smartphones, tablets, laptops, notebooks, and even more devices that weren't even in the picture only a few years ago.

These reasons provide compelling justification for the dramatic shift toward cloud computing—its flexible

delivery model alone has the capability to completely remake your business into a more dynamic and profitable enterprise, perhaps even saving you money in the process. More than any other improvable aspect of your business, cloud computing has the power to transform your company by delivering state-of-the-art applications, engaging users more fully, enhancing the online experience, and making optimum use of the most modern online devices.

This collection of attributes has the potential to completely level the playing field for your company, allowing you to compete against much larger corporations by achieving an optimal online presence and establishing your brand on an equal footing with the giants of your particular industry.

In this chapter, we'll look at what you need to know about cloud security and computing, if you haven't already made the leap of faith it requires, and we'll survey the security aspects of cloud computing so you can understand how the risks might be different from your in-house computing. Finally, we'll consider how you can secure your company's most valuable data assets while using the cloud, thereby gaining all the benefits while minimizing risks involved.

Cloud Computing—What You Should Know

The first thing to know about cloud computing is that it has now become the overwhelming champion of strategic technology around the globe and is estimated to approach $200 billion in value as an industry by the year 2020. This isn't just an accident of course—the cloud computing market has been dramatically powered like this by the

business need for flexibility, speed, and universal access from any location, by any device. Because the cloud has so much to offer, its appeal has already soared to the forefront as a transformer of businesses.

But that's just the beginning. Having already delivered the tools to help drive complete business transformation, the cloud is now quickly becoming the enabler for process improvement, as well as for providing an enhanced and more engaged customer experience. As if there were any doubt, a survey recently conducted by KMPG documented that close to one thousand leaders in the technology industry consider cloud computing to be the single most pervasive technology in changing the way companies do business over the next several years.

Cloud computing has the capability to affect almost everything about the way you do business and to improve on what you've been doing by providing efficiency gains and more creative approaches. The KMPG survey emphasized that some of the business areas currently being altered dramatically by cloud technology are data analytics, total cost of ownership, greater alignment between customers and business personnel, empowerment of the mobile workforce, faster time to market, and a pronounced movement toward global business models.

Here's a key thing to understand about cloud computing: It isn't simply a platform that will allow you to do what you're doing in a better way (although it does that), but it is poised to become the foundation upon which future innovation will be built for some time to come. It's not just

about cost savings and efficiencies; it is an enabler for the most advanced new technologies on the horizon, and if your company can embrace these new technologies and make them part of your business, it will go a long way toward keeping your business competitive and possibly gaining a step on your rivals.

What About Security On The Cloud?

Right from the beginning, security has been a kind of fly in the ointment for cloud computing and the one objection most commonly tendered by businesspeople considering a move toward the cloud. As opposed to the supposed safety of keeping valuable data assets in-house and under the protection of motivated company employees, it seemed like inviting vulnerability to have critical business information be repositioned on servers somewhere else, under the care and management of people who have no personal interest in its safety.

Are there risks associated with migration to the cloud? Absolutely. However, from the above it should be apparent that the enormous advantages offered by cloud computing far outweigh any risks involved in moving to that platform. The truth is that your business data is no safer in-house than it would be on the cloud and no more at risk. Cybercriminals are out there, and they'll find you and your business whether you're on the cloud or whether you've battened down the hatches of your own standalone computing environment, thinking about how safe and

secure your business is. If you're connected to the Internet, you're at risk.

The Four Major Assailants of Your Network

Bear in mind that these four categories of data asset attackers do not operate solely against cloud-based businesses; as stated above, your business data is no safer from a determined cybercriminal within the walls of your own building than it would be on a server farm somewhere on the cloud. Attackers couldn't care less about physical location—all locations represent a source of income to them.

That being said, here are the four categories of the greatest security threats in operation today: *cybercrime*, *cyberespionage*, *hacktivism*, and internal *employees*. You may be a bit startled by that last category, so let's tackle it first. In a study published by the *Wall Street Journal* recently, it was announced that as many as 75 percent of all employees take advantage of the opportunity of stealing data from the company they still work for or have recently left.

This can involve stealing lists of customers, research information from an R&D department, or even managers taking any kind of information with them that might help at a new job. Maybe you haven't thought of your own employees as a security threat before, but who has better opportunity than someone does on the inside? Hackers spend all their time trying to penetrate security defenses and get inside—internal employees are already there.

Hacktivism may also be a bit of a surprise and is perhaps a term you aren't really familiar with. This form of attack has come to light in recent attacks against SONY, which was apparently targeted for political reasons by a group sponsored by North Korea, in retaliation for a SONY movie portraying that country's leader in an unflattering light. Apparently bent on making a statement to the world, these hacktivists secured their desired headlines by hacking into the computer systems of those companies. This form of attack does not appear to be motivated by monetary gain, but it is simply to announce the power of the attacker and to put a global spotlight on their political or social agenda.

Cybercrime, by contrast, has been around for quite a while and is still enormously popular because it is so difficult to prevent and because the rewards are so significant for attackers. Credit-card theft comprises the majority of such attacks for obvious reasons, but there are also thefts of insurance data, e-mail addresses, and medical records, which can be used to leverage financial gain for the cybercriminals.

Cyberespionage is often used by commercial rivals or is a state-sponsored criminal activity that seeks to gain entrance to networks containing intelligence information to be used for political advantage or to gain leverage with international dealings. China and Russia are major players in this arena, but they are by no means the only players.

How Cybercriminals Breach Your Defenses

At the outset of this discussion, you should realize that the simple and somewhat disturbing truth is that security is not nearly so much a technical problem as it is a *people problem*. If employees were better trained with an understanding of how security really works, there would be far fewer breaches of networks, and cyber attackers would be a lot more frustrated than they currently are. As it is, cyber attackers are well aware of the fact that the *weakest link in any network is almost always the people* who administer it and access it on a daily basis. Besides the human-based vulnerabilities, there are also some technically oriented aspects of security threats.

The latest and greatest malware: Robotic malware currently rules the roost when it comes to compromising computer systems. “Bots,” as they are called, commonly get installed on your computer when you open infected attachments and e-mails or download infected files from websites.

Mobility trends: Many employees don’t think twice about storing company data on their smartphones or other mobile devices, creating a blurry line between work and personal lives. Potentially sensitive data can thus easily be stored and transmitted from mobile devices with no real thought about security.

Social-media vulnerability: The use of social media[1] has become so prevalent, even during work hours, by employees that many employees give no thought at all to revealing sensitive information about themselves or their company in chat sessions. A number of attacks have been reported where men have freely given up company information—even including passwords—to especially friendly female chat partners who turned out to be clever male hackers.

Cyberterrorism: Highly capable hackers now have the ability to take down entire power grids and hold other components of infrastructure hostage in order to achieve their objectives.

False sense of compliance security: Many companies make legitimate efforts to become compliant with security standards, and once they achieve that, they simply stop working on security or worrying about it at all. In actuality, most compliance rules are only intended to set a company on the path toward security but not to actually address the underlying issues with security. This explains why companies that may be in full compliance with security standards get hacked all the time.

Advanced persistent threats: Also known as APTs, advanced persistent threats are network attacks in which an

1. "Why Hackers Love Companies Who Use Social Media"/Sue Poremba/Forbes/FEB 24, 2015 @ 08:00 AM/ http://www.forbes.com/sites/sungardas/2015/02/24/why-hackers-love-companies-who-use-social-media/#4a09a78a4dfb.

unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause immediate damage to the network or organization.

Internal threats: With practically every successful cybercrime carried out, there is an internal breach at the bottom of it. This may be an intentional compromise such as accepting a bribe or a completely unintentional weakness exposed by an employee through sheer ignorance.

Security on the Cloud versus In-House Security

As previously mentioned, your business data is not entirely safe from attack no matter where it is physically located, so for the most part, there is no greater threat to your valuable information assets on the cloud than on your own premises. However, there are some issues specific to the cloud that should be considered, such as where it's actually stored, who has access to it, and what kind of regulatory measures govern maintenance of it.

Whereas on your premises you have complete control over your data and all access to it, on the cloud you never really know where it's stored or who can access it. Because you never really know where your valuable information is being stored, there's no foolproof way to understand how it's actually being managed on your behalf. The nature of cloud services dictates that data is highly distributed and very much virtualized so that your company's data could

actually be physically located almost anywhere in the world, subject to those locations where your cloud provider has a physical presence.

Since your data would reside on the cloud, anyone who can access the cloud would theoretically have access to it, and it could "leak" into other companies' data simply by virtue of physical proximity. Granted, a cloud provider would take steps to minimize this risk in its management processes, but it is a risk nonetheless.

In addition, your company data could actually be located somewhere in the world that has relatively weak laws protecting the intellectual property rights of your data. This puts the onus on you and your company to have a thorough understanding of important contract points with your cloud provider and to understand exactly where your data will be stored and who has access to it. The time to bring all this up is during negotiations with your provider, at which time you should insist on an arrangement that you feel comfortable with and that will ensure the ongoing protection of your company's most valuable data assets. Something that might provide you with an increased comfort level would be to include a provision for allowing greater visibility by having a third party audit your cloud provider periodically.

Another issue specific to the cloud platform is that of data availability, and by this, I mean having round-the-clock daily access with no downtime. Of course, downtime would be just as possible on your own premises if you had a sudden hardware or software failure, but in that situation,

you'd be in complete control of any recovery effort, which means presumably pulling out all stops to get back online quickly.

As a matter of fact, you probably even have some kind of redundant network configuration for just such occasions, and at the very least, you should have backups from the prior business day. On the cloud platform, there are no guarantees to cover these situations, unless they are stipulated in the terms of a contract with your provider.

What happens if the Internet connection to your cloud provider goes down? This is another situation where it's really up to you to make sure the scenario is covered somehow by the terms of your agreement and that a downed connection can be remedied either by a redundant line or by a guarantee of recovery within an acceptable time frame. This will come with a trade-off though—you would almost certainly incur increased costs for the privilege of having a redundant line or recovery guarantee.

Migrating to the Cloud

By 2020, more than 80 percent of all businesses will be on the cloud, so if you're not there yet, chances are you will be within just a few years. If you haven't given it your full attention yet, now is as good a time as any. But don't just give it a cursory examination. Consider it within the framework of issues that are really critical to your business.

Your company's most valuable data assets: Conduct a thorough assessment of where your valuable company data currently resides, for instance, on the network, on employee desktops and laptops, and possibly even on mobile devices. Do you have a policy in place for backing up all this critical information somehow, and are those backups immediately accessible when needed?

Applications: Identify the applications that are most critical to daily productivity by your employees and determine what the impact would be if you lost access to these applications for any amount of time.

Appeal of your data: Consider who would benefit by having your company data and the potential avenues they might use to get at it.

Preventing data breaches: Along with the understanding of what the most likely paths are for breaching your system and how such breaches might be prevented, you should think about the human vulnerabilities. Part of this is being

honest about how well trained your employees are at recognizing threats and not falling into traps set by cyber attackers.

The point of all this heavy-duty thought is to get a feel for how much risk is associated with migration to the cloud for your company. Although the tremendous benefits of cloud-based computing have been prominently lauded earlier in this discussion, not all of them apply to every business, and it might very well be that the actual benefits your own company would derive are not all that significant.

If your company is not one that thrives on innovation and doesn't use the most modern tools and technologies, the appeal of the cloud will probably be considerably less for you. In any case, weighing the benefits achievable with cloud-based computing against the potential risks you identify for your company should provide you with a fairly clear answer as to whether migration to the cloud is in your company's best interests.

No matter what you do, security will still be an important part of your business, even if most of your data and most of the applications used by your company are situated on the cloud platform. You still have to maintain in-house security for local applications, and you still have employees who are vulnerable to clever cyber attackers.

Security is so interwoven throughout the fabric of modern computing that there is no such thing as simply farming out your data, your applications, and all the security measures it takes to protect them. Wherever computing is done, good security practices such as regular user training and monitoring threat intelligence will be necessary.

Chapter 8: Hackers

A lot was written about this subject, and it is covered by various certifications. It may be important to profile hackers to know how to protect ourselves. Since this book is focusing on the business side rather than the technical, I will include a short description for each.

Hacktivist

This type of attacker is looking to grab our attention to social or political agendas.

White-Hat Hacker

This person is used by many companies to act as the hacker breaking in to a given system. The problem with this approach is that often his or her scope is very *limited*, whereas a bad hacker is not, which in turns brings no true results of the exposure and attack impact but *is* required by all compliance programs such as PCI DSS.

Black-Hat Hacker

This person is spending his or her time hacking into systems mostly for financial gain.

Nation-State Hackers

North Korea, Iran, Russia, and China are top courtiers who attack and hack systems for intellectual property, army espionage, financial systems, energy, and the critical infrastructure targets. They can go after private companies if they see a great fit for their objectives. Another option is to change or skew political views of the public by publishing e-mails, as was the case with WikiLeaks.

The Insider

This person can be an employee who will sell his or her workplace information for a few hundred dollars to a potential hacker, as happened using social media.

Regardless who is the attacker and/or his or her motives, it's important to know what you are trying to protect. Would you know if someone accessed a certain file or if this file was copied and then deleted?

Recent research conducted by the Ponemon Institute in August 2016 found that 76 percent of companies have experienced the loss or theft of company data over the past two years. That's an increase of 11 percent from a 2015 survey.

It's time to monitor!

Chapter 9: The Silent Assassins

Your IT people may not see evidence of foul play, but inside every network, we will find major issues. In some cases, the data caretakers have become numb to these problems. They are everywhere; the thought is that they are not hurting us. The IT team is wrong about this. Let's look at some references from the news.

"Executives were told the networks aren't connected…it's not entirely true."—Wall Street Journal.

Isn't that so often the case—senior management is in the dark on how things are connected! — Wall Street Journal

"On average, malicious software infections are not discovered for 15 months, according to ICS-CERT. That leaves hackers plenty of time to do damage."—Wall Street Journal

"When they hack into a system, they do have the ability to crush the system…I think they are there to steal the data."—Wall Street Journal

"More than 90 percent of user-generated passwords, even those considered strong by IT departments, are currently susceptible to hacking."—Deloitte's analysis

"*The stock of pacemaker manufacturer St. Jude Medical Inc. (STJ.N) fell sharply on Thursday after short-selling firm Muddy Waters said it had placed a bet that the shares would fall, claiming its implanted heart devices were vulnerable to cyberattacks.*"—Reuters

Computer Virus

A virus is a software package that was written by people who are looking to cause damage. In the simplest definition, a computer virus acts the same as a human virus does; you need means and contact to make it spread.

Years ago, we had floppy disks to spread them, so their impact was very low and the damage was not the same as today. Nowadays, malicious software can spread via e-mail attachments, USB drives, webservers, wireless, and websites.

Malware and Bots

A bot or robot is a software application that is mostly used to scrap data off Internet resources, that is, websites. For instance, you can scrap websites for e-mail addresses that later on will be used to create spam campaigns.

Malware is also a software application that will do everything to hide its activity while causing damage by consuming Internet speeds, locking down files, and asking for a ransom.

The next step can be a combination of malware and a bot residing on a computer network for a long time while scrapping data and uploading your information outside your network.

Malware can reside on your mobile devices, such as tablets and smartphones, using the same concepts as described above.

Wait! This is getting even better, infecting your car, freezer, lights, smart home, and so on.

The Most Powerful Attacking Tool Available Now

Social engineering is *the* number-one method of getting in without even knowing. Security is *not* a technology problem; it's a *people problem.*

The risk with this medium of communication is that there is minimal control, and a bad post, a hack, or an incorrect statement can make the organization look inexperienced and offensive at worst. Furthermore, social media provide more information about the employees and their functions, which can be useful information for someone who is trying to socially engineer a hack.

If you read Kevin Mitnick's book *The Art of Deception*, you will discover some great stories about how easy it is to get in, sneaking into military, financials firms, or any gated location simply by talking to the right people using some known names and the same terms/language. The main point here is that people trust people they know. Nowadays all

this information is available from websites and social-media profiles.

Office workers are overloaded and need to get the job done. Few will question; it's easy to comply and help a "coworker" do his or her job as well.

When social engineering is used as a part of a vulnerability assessment or pen test, it will be successful. The question is what can be done to minimize this threat?

Companies that have a security policy in place and talk about it are better off because they acknowledge the risk. Employees are aware of the risk, and that awareness translates into better security. Smart users will use technology more securely and better understand the ramifications if they do not apply best practice in social-media outlets.

Social-media security also requires good security tools. The volume and complexity of regulations, policies, and posts are such that the only way to approach social-media security and compliance is by using technology augmentation: computerized systems that can scan and process information faster and more consistently than any department or outsourced service full of people. Only people and processes combined with technology guardrails can safely and effectively address this security challenge.

Chapter 10: Risk Management

As a businessperson, you weigh risk versus gains. Even a non business person will need to have this straightforward approach. For instance, renting versus buying a house. This is somewhat simple. Data security, on the other hand, is not that simple, as you cannot really measure it or at least don't know or don't have a measuring stick—yet.

How to Measure Your Risk

You need to have a clear understanding of applicable threats and data assets and how likely a threat will be realized and what will be the impact of a network breach. You can't really protect what you do know if you have already been hit.

One Friday night after having our family meal and putting our three kids in bed, my wife and I finally landed in bed. During the entire night, I did not feel very well as some unrest was going on in my stomach. As an Israeli, I don't take these things seriously (unlike my wife) enough and thought this may go away by itself. As I was turning in my bed, I was busy with calculations if I should get up and go to ER, but that would scare the kids and wife, so I delayed my decision. Finally, I woke up my wife and explained the situation. Immediately, she called for an ambulance. The team asked me a few questions while checking me; I was

rushed to the hospital and admitted. After running some tests that all came clear, I was ready to go home because after all, the likelihood of danger was very low now—there was no risk. The doctor asked me to stay for the night just to be sure nothing was wrong. While we had our discussion, he decided to run another test checking my kidneys, and there were no signs of stones. He suggested further testing with my family doctor. I must admit that I did not do anything to this day. I'm not a fan of hospitals and doctors.

The next morning, I felt much better and waited for a taxi to pick me up after a long night of a snowstorm.

The reason I decided to go to the ER was determined by high impact and a high likelihood that something may happen or was going on that I was not aware of.

How to Use Your Measuring Stick before You Can Make a Decision on How to Protect Data Assets

The impact will be determined by your data value; a higher data value means higher the impact. Personal information like SSN has a higher value than just work e-mails (not always).

The likelihood is determined by the exposure of that data; internal and external users, mobile devices, laptops, Internet café, and public networks represent a very high exposure, hence a higher likelihood.

Your graph may look like this.

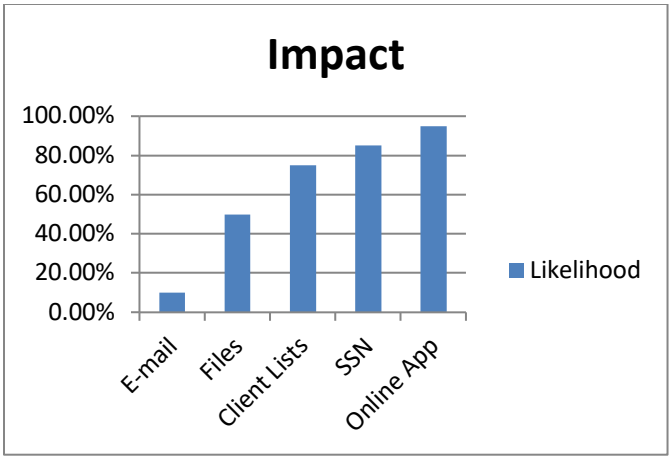

Table 4. Impact versus Likelihood

Here's how I do it; with every business owner, we take the time to ask three fundamental questions about his or her current security posture:

1. What are you trying to protect?
2. What are the relevant threats?
3. How comfortable are you with your ability to detect and respond to cyber incidents before it's too late?

Now, let me explain; the above questions will help you map out data types and their locations (or where it is stored). Then we want to know what is relevant to your company, industry, business partners, customers, suppliers, and employees. Next, we ask if you discover a potential threat within your systems, how quickly you can find it and remove it.

The purpose of the above three questions is to raise your awareness and thinking process about how vulnerable you may be by setting the stage for a fix.

This process can take time, and some business owners and managers don't like that. As someone noted, "You asked a lot of questions," which showed him that he is in a *bad* shape (his company was hacked twice).

Let's go over a scenario.

Question number one drives the impact; the more data types, the higher the impact. Let's say you store SSNs, credit-card numbers, and Excel sheets with customers' information and patents. If a data breach were to happen, all that information may be exposed to an attacker.

Question number two drives the likelihood. The more threat actors, the higher the likelihood. Suppliers have access to your data over the cloud and malware that can steal files and then encrypt data and so they can ask for a ransom to rollback.

Question number three: No, we won't know if someone touched a file, and we are not comfortable with what we have to discover cyber events. This is the *one* area where most businesses fail.

You Should Make a Note to Yourself

Now this fictitious business scenario gives us high impact with medium to high likelihood to happen. The impact would be much higher if you don't know what's going on.

Are you a sitting duck?

Chapter 11: Tech Trends: Bonus Chapter

As a business owner, you should be aware of upcoming technologies and trends that may have the potential to put you out of business before you even know it. For instance, Google makes changes to its search-engine algorithm; it turns out, the search results may not show your business listed as it was before.

Predicting the advances in technology even a decade into the future can be a precarious undertaking since so much can develop very quickly, but predicting the technology for the coming year is on somewhat safer ground. While many people simply wait to be surprised by the latest gadgets and devices, others enjoy making educated guesses based on current trends and news stories. If you have any thoughts on emerging technologies in the present year, compare them to the predictions listed below.

Virtual-Reality Advances

Virtual-reality headsets will really take off, with Oculus offering a new product called Rift, which will make it possible to "experience anything, anywhere." Google is also developing a whole range of headsets to compete in the market with the established players.

Wearables

It is estimated that around forty-five million adults in the United States will be making use of wearables in 2020, including fitness trackers and smart watches. Usage has been soaring ever since their introduction a decade ago, and interest is probably still not yet peaking.

Internet of Things (IoT)

More and more devices will be connected to the cloud, increasing their functionality and improving their responses to real-time situations. Smart cars and wearables will also be connected, making them much more capable than they otherwise would be.

Artificial Intelligence

After decades of stagnation, artificial intelligence is finally poised to take the proverbial quantum leap due to three critical advances: cheap parallel computation, big data, and much better intelligence algorithms.

Payment and Currency Systems

Digital technology is paving the way for new forms of payment and currency systems, including the mobile wallet, wearables like the smart watch (see above), pay-by-fingerprint, and even tweets and texts.

Three-Dimensional Printing

Three-dimensional printing machines will be capable of "printing" almost any design conceivable by a consumer by creating single, wafer-thin slices of that object at a time, layered to comprise the whole object.

Cybersecurity

Cloud services are changing rapidly as more customers are transferring data assets, making a huge impact on current and future data-protection technologies. Companies that used to own and manage their data centers had a simple task of protecting their companies' perimeter, but now the broad use of cloud services leaves enterprise data vulnerable to theft.[2]

2. Broad use of cloud services leaves enterprise data vulnerable to theft/Patrick Nelson/NETWORKWORLD/JAN 25, 2016 1:25 PM PT http://www.networkworld.com/article/3025944/security/broad-use-of-cloud-services-leave-enterprise-data-vulnerable-to-theft-report-says.html.

Integration of All the Above

Taking each of these advanced technologies to the logical next level, they will be integrated with each other and with the cloud, thereby multiplying their functionality. However, this will also have the effect of blurring traditional borderlines, making data privacy and data security even more challenging. Data assets will become targets of the fertile minds of hackers, necessitating corresponding advances in cybersecurity along with device technology.

Appendix A: Buzzwords and Tech Talk

It's essential to understand how tech people talk, so you won't be sitting in meetings with IT, nodding your head as if you get it, but it actually sounds like some alien conversations, while you are trying to get real answers about the business. Is it going to improve revenue, customer service, save expenses, increase the bottom line?

Access control: A procedure to identify and/or admit personnel with proper security clearance and required access approval(s) to information or facilities using physical, electronic, and/or human controls.

Advanced persistent threat: APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.

Application: Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

Authentication: Security measure designed to establish the validity of a transmission, message, originator, or means of verifying an individual's authorization to receive specific categories of information.

Bot: A computer connected to the Internet that has been surreptitiously/secretly compromised with malicious logic to perform activities under the remote command and control of a remote administrator.

Cloud computing: A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Compliance: It seems like everyone wants to have his or her company become compliant with all types of rules and regulations meant to keep data secure. That's a good thing. But for many companies, "compliant" is doing the bare minimum toward data security while claiming the company meets regulatory standards. Real compliance is an ongoing process to do everything possible to prevent breaches and other threats.

Configuration control: Process of controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during,

and after system implementation. See: Configuration management (CM).

Configuration management (CM): A discipline applying technical and administrative direction and surveillance to

1. identify and document the functional and physical characteristics of a configuration item,
2. control changes to those characteristics, and
3. record and report changes to processing and implementation status.

Critical infrastructure: The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Cyberspace: The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems and embedded processors, and controllers.

Cyberattack: A hostile act using computers or related networks or systems intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of a cyberattack are not necessarily limited to the targeted computer systems or data themselves—for instance, attacks on computer systems that are intended to degrade or destroy the infrastructure of command and control (C2) capability. A cyberattack may use intermediate delivery vehicles including peripheral devices, electronic

transmitters, embedded code, or human operators. The activation or effect of a cyberattack may be widely separated temporally and geographically from the delivery.

Cryptography: Art or science concerning the principle's means and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form.

Data: Information, regardless of its physical form or characteristics, that includes written documents, automated information systems (AIS), storage media, maps, charts, paintings, drawings, films, photos, engravings, sketches, working notes, and sound, voice, magnetic, or electronic recordings.

Data breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Digital forensics: The process and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

Data loss prevention: "DLP" is often the term used to describe the last point of defense against a data leakage, but it is actually the strategy and software the security team develops to protect data.

Denial of service (DoS): When an action(s) results in the inability to communicate and/or the inability of an automated information system (AIS) or any essential part to perform its designated mission, either by loss or by degradation of a signal or operational capability.

Digital signature: A cryptographic process used to assure message-originator authenticity, integrity, and nonrepudiation. An electronic signature that is a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:

1. whether the transformation was created using the private key that corresponds to the signer's public key, and
2. whether the initial message has been altered since the transformation was made.

Endpoint protection platforms *(EPP)*: Gartner's *Magic Quadrant for Endpoint Protection Platforms* report explains that endpoint protection platforms as "a solution that converges endpoint device security functionality into a single product that delivers antivirus, antispyware, personal firewall, application control and other styles of host intrusion prevention (for example, behavioral blocking) capabilities into a single and cohesive solution." It's an essential need for information security, as every device we use—from our computers to smartphones—is considered an endpoint and needs to be secured. The problem it helps to solve is protecting the overwhelming number and types of devices now being connected to networks.

Enterprise risk management: A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

Hard disk: A magnetic storage device used for high-volume data storage and retrieval purposes to include ones that are both removable and not removable from the computers in which they operate.

Information assurance: The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.

Insider threat: Any circumstance or event with the potential to adversely impact agency operations, including mission, functions, image, or reputation; agency assets; or individuals through an information system (IS) via internal unauthorized access, destruction, disclosure, modification of information, and/or denial of service (DoS).

Intrusion detection: The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

Malicious code: Software or firmware that is designed with the intent of having some adverse impact on the confidentiality, integrity, or availability of an information system. The malicious code may be included in hardware, software, firmware, or data. Computer viruses, worms,

Trojan horses, trapdoors, and logic bombs all fall under the definition of malicious code. Computer viruses pose the primary threat to an IS because of their reproductive capability.

Malware: Software that compromises the operation of a system by performing an unauthorized function or process.

Passive attack: An actual assault perpetrated by an intentional threat source that attempts to learn more or make use of information from a system, but it does not attempt to alter the system, its resources, its data, or its operations.

Penetration testing: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Ransomware: This is malware, but it is a very specific type of malware that requires some sort of ransom payment either to remove the malware or to retrieve files that have been encrypted by the malware. Ransomware has been around for a long time, but it made news this year when WannaCry encrypted files and then demanded payment in Bitcoin.

Risk assessment: A written evaluation supporting the adjudicative process, especially when a significant exception to a personnel security standard is being considered. This assessment should consist of an evaluation from security, counterintelligence, and other technical or management experts as appropriate, and it should contrast the compelling national security benefit of an individual's access to sensitive compartmented information (SCI) with the risk. See: Risk management.

Risk management: The Information Systems Audit and Control Association describes it this way: "Information risk management defines the areas of an organization's information infrastructure and identifies what information to protect and the degree of protection needed to align with the organization's tolerance for risk. It identifies the business value, business impact, compliance requirements, and overall alignment to the organization's business strategy. Once this information has been identified, it can be presented to the business leadership to make decisions about the level of investment (both financial and resource) that should be utilized to create appropriate information protection and risk management capabilities."

Threat: Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or Denial of Service (DoS).

Threat analysis: An operations security (OPSEC) process that examines an adversary's technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities. See: Threat assessment.

Threat assessment: An evaluation of the intelligence collection threat to a program activity, system, or operation. See: Threat analysis.

Threat monitoring: The analysis, assessment, and review of information system (IS) audit trails and other data collected for the purpose of searching out system events that may constitute violations or attempted violations of data or system security.

Trojan horse: A computer program with an apparently or actually useful function that contains additional or hidden functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security (e.g., making a "blind copy" of a sensitive file for the creator of the Trojan horse). See: Malicious code.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability analysis: A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might undermine critical information in time to disrupt or defeat the operation or activity. See: Vulnerability assessment.

Vulnerability assessment: The result of a vulnerability analysis expressed as a degree of probable exploitation by an adversary. See: Vulnerability analysis.

Whitelist: A list of entities that are considered trustworthy and are granted access or privileges.

Worm: A worm is a program, originally developed by systems programmers, that allows the user to tap unused network resources to run large computer programs. The worm would search the network for idle computing resources and use them to execute a program in small segments. Built-in mechanisms would be responsible for maintaining the worm, the worm finding free machines, and replicating the program. Worms can tie up all the computing resources on a network and essentially shut it down. A worm is normally activated every time the system is booted up.

Appendix B: Q&A

This section is written to educate you about some areas that you may see on reports, hear in meetings, and hear in conversations in your company and on the news and never had the courage to ask. I will explain what information security is and what are some myths and facts.

It's written for nontechnical people or business management and/or executives. If you are already familiar with this information and network security, you may wish to simply skim this section.

What are network and/or information security?

Before you can understand the concept of network security, you must decide what security means to you and your company. Perhaps to you, feeling secure means knowing that you are safe from any outsider gaining access to your confidential files and private company information. If this is the case, use this policy to evaluate what goes on with your network because the same private information is also stored in your computer systems.

Network security simply means preventing unauthorized use of your computer network. Taking the necessary precautions to protect your network will help to keep unauthorized users, or hackers, from gaining access to your computer system or network.

Network security can also assist you in detecting whether a hacker tried breaking into your system and what damage, if any, was done.

When it comes to network security, most companies fall somewhere between two boundaries: complete access and complete security. A completely secure computer is one that is not connected to the network, not plugged in, and physically unreachable by anyone. Obviously, a machine like this does not serve much of a purpose in your office.

On the other hand, a computer with complete access is very easy to use, requiring no passwords or authorization to provide information. Unfortunately, having a machine with complete access means anyone could access it. This could spell disaster for you and your organization.

Why is network security so important?

You may have a good understanding of what network security is, but you may not know why it is so important. Being educated about what a hacker may be looking for on your system can help you understand why keeping your network secure is so critical.

There are several reasons for keeping your information secure. Of course, the obvious reason that most people consider network security so important is to keep hackers away from their personal information. Intruders can gain access to your financial records, confidential client

information, and private company data. However, this is not the only reason for security.

Most of us probably would not consider our communications and files to be top-secret information, but this does not mean we want others reading it. Many people believe if they use only their computers to send e-mail, surf the Internet, or play computer games, they will not be targets for hacker attacks. Beware! Hackers may not care about your personal information; they may want to get into your network so they can attack other systems while making the attacks appear to be coming from you. Having this control over your network will enable them to hide their own identity. This could create a liability for your business, potentially even involvement in a federal investigation.

Investing in a high-quality firewall is a good start to securing your network, but it is important to understand that firewalls are not threat-free. Having the best lock on your front door does not necessarily mean you will never be robbed. Likewise, having the best firewall does not automatically mean you will never be a victim of a hacker attack. It simply means that a hacker only has one thing to break to gain access to your entire network.

Hackers are discovering new vulnerabilities every day. Unfortunately, computer software is so complex that it is nearly impossible to ensure it is completely free of errors. Software vendors will often develop patches to address these errors after they are discovered. However, it is generally up to the user to find the patches and install them on their own computers.

Ten Assumptions and Facts about Network Security

Many people and businesses unknowingly leave their private information readily available to hackers because they subscribe to some common assumptions about computer and network security.

Below are ten assumptions and their facts:

Assumption 1: "I have virus-protection software so I am already secure."

***Fact*:** Viruses and security threats are two completely different things. Your antivirus software can only protect you from past known attacks/viruses and not every time. Only vulnerability assessment will test your network, such as whether your financial or customer records are exposed to the Internet or whether your computer is vulnerable to various hacker attacks.

Assumption 2: "I have a firewall, so I don't need to worry about security threats."

***Fact*:** Firewalls are great and typically provide a good layer of security. However, firewalls commonly perform services such as port forwarding or network address translation (NAT). It is also surprisingly common for firewalls to be

accidentally misconfigured. The only way to be sure your network really is secure is to test it.

Assumption 3: "I have nothing to worry about; there are too many computers on the Internet."

***Fact*:** People understand the need to lock their homes, roll up their car windows, and guard their purses and wallets. Why? Because if you don't, then sooner or later, you will be a victim. However, people are just starting to be aware that the same is true with their computers and networks. A single hacker can scan thousands of computers looking for ways to access your private information in the time it takes you to eat lunch.

Assumption 4: "I know the security of my network and information is important, but all the solutions are too expensive and/or time consuming."

***Fact*:** While it is true that some network-security products and services are very expensive and time consuming, investing now will save you more!

Assumption 5: "I can't do anything about my network's security because I don't know how to."

***Fact*:** My company can consult you by assessing your specific needs and relevant threats; we will help you to improve your network security as well as your knowledge.

Assumption 6: "I know what is running on my computer, and I am sure that it is secure."

***Fact*:** You may not know that you have been infected while on the Internet, by some attacker having installed a rootkit on your machine, leaving you with no ability to trace it or even remove it.

Assumption 7: "I tested my network a few months ago, so I know it is secure."

***Fact*:** New security threats and vulnerabilities are discovered on daily basis. Security threats are being discovered constantly, so testing and monitoring is needed to counter these newly threats.

Assumption 8: "Network and computer security is only important for large businesses."

***Fact*:** In reality, nothing could be further from the truth. Whether you are a casual home user or a large enterprise, your computer contains valuable and sensitive information.

This could be financial records, passwords, business plans, confidential files, and any other private data.

In addition to your private information, it is also important to protect your network from being used in denial of service attacks, as a relay to exploit other systems, as a repository for illegal software or files, and much more.

Assumption 9: "A 'port scan' is the same thing as a security analysis scan, and some websites already give me that for nothing."

***Fact*:** Actually, a port scan and a security-analysis scan are two very different things. In general terms, your computer's Internet connection has 65,535 unique service ports. These ports are used both by software running on your computer and by remote servers sending data to your computer (when you view a web page or check your e-mail).

A port scan will simply tell you which service ports are being used on your computer. It does not test any of these ports for security threats, nor does it tell you where your network is vulnerable to possible hackers or attacks. 2Secure Corp. will perform a port scan as a small part of a vulnerability assessment to find possible security threats.

Assumption 10: "The best time to deal with network security is when a problem arises."

Fact**:** The best time to deal with network security is *before* a problem arises, to prevent you from ever becoming a victim. Think about it—the best time to lock the doors in your home is before a robbery occurs. Afterward it is already too late; the damage has been done. This is why it is critical to analyze your network's security now, to find and fix the vulnerabilities before a break-in happens.

Appendix C: Sources

[1] Sue Poremba. Forbes. *Why Hackers Love Companies Who Use Social Media*. FEB 24, 2015 @ 08:00 AM http://www.forbes.com/sites/sungardas/2015/02/24/why-hackers-love-companies-who-use-social-media/#4a09a78a4dfb.

[2] Patrick Nelson. NETWORKWORLD. *Broad use of cloud services leaves enterprise data vulnerable to theft.* JAN 25, 2016 1:25 PM PT http://www.networkworld.com/article/3025944/security/broad-use-of-cloud-services-leave-enterprise-data-vulnerable-to-theft-report-says.html.

Appendix D: Other Resources

The following Internet sites contain valuable information and system patches that you may find useful to improve your information-security knowledge

• CERT Coordination Center—The CERT/CC is one of the major reporting centers for vulnerabilities and security incidents. It is a federally funded research and development center, which was created in 1988 in response to the "Morris Worm." The center is operated by Carnegie Mellon University and is a valuable resource for descriptions of security vulnerabilities, information on vendor patches, and system-configuration guidelines.
Url: http://www.cert.org/

• CVE Database—The Common Vulnerabilities and Exposures (CVE) list provides a set of standardized names for computer vulnerabilities. The website is hosted by the MITRE Corporation and is funded by the US government.
Url: http://www.cve.mitre.org/

• Microsoft Security—Microsoft Security Advisories.
Url: http://www.microsoft.com/security

• Sun Microsystems—Sun Security.
url: http://www.sunsolve.sun.com/

• Red Hat Security—Red Hat Linux Security.
url: http://www.redhat.com/solutions/security

• Cisco Systems—Cisco Security.
url: http://www.cisco.com/

• Apache Web Server—Apache Software Foundation provides one of the most popular web servers in the world.
url: http://www.httpd.apache.org/

• OpenSSH—OpenSSH is a popular implementation of the Secure Shell protocol.
url: http://www.openssh.org/

• OpenSSL—OpenSSL is a popular implementation of the Secure Socket Layer protocol.
url: http://www.openssl.org/

• Oracle—Oracle Security.
url: http://www.oracle.com/solutions/security

• MySQL—Popular open-source database, especially in web-hosting centers.
url: http://www.mysql.com/

• PHP—Popular web programming language.
url: http://www.php.net/

• Trend Micro—Antivirus vendor and virus information.
url: http://www.trendmicro.com/

• McAfee Security—Antivirus vendor and virus information.
url: http://www.mcafee.com/

When You Fall Victim To A Cyber-Attack Through No Fault Of Your Own, Will They Call You Stupid...Or Just Irresponsible?

Its EXTREMLY unfair, isn't it? Victims of all other crimes – burglary, rape, mugging, carjacking, theft – get sympathy from others. They are called "victims" and support comes flooding in.

But if your business is the victim of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will be instantly labeled as stupid or irresponsible. You will be investigated and questioned about what you did to prevent this from happening – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders.

Yigal Behar is a seasoned Cyber Security professional with over 32 years under his belt, Mr. Behar parlayed his experience consulting for high-profile entities like the Israeli Prime Minster Office and other governmental agencies, banks such as Bank Hapoalim into his entrepreneurial pursuits. In 2003, he launched 2Secure Corp, his second venture, and has since dedicated himself to its growth and success. He believes in personalized client engagement, leveraging his expertise and business development skills to deliver custom solutions.

To share his cybersecurity expertise and guide small and medium-sized business owners and managers, Mr. Behar launched "The Cybersecurity Insider" podcast. Tune in on YouTube for valuable insights and guidance. Don't miss out on valuable tips - subscribe today!