Cyber Talk

SECURING YOUR CYBER ECOSYSTEM:

STRATEGIES FOR BUILDING POWERFUL RESILIENCE

TABLE OF CONTENTS

INTRODUCTION

Sophisticated cyber threats are skyrocketing, with 3.9 trillion intrusion attempts reported globally within the past year.[1]

Due to the high volume of threats, and the magnitude of the business impact, cyber security is no longer just an IT issue. Executives and board members need to take note as well. Become an informed business leader so that you can strengthen your organization's cyber security posture.

This eBook is designed to enrich your knowledge and expand your perspectives so that you can proactively avoid cyber damage, find the right protection for your business, and outsmart the hackers.

> "Increased cyber risk is real - but so are the data security solutions."
> –Gartner[2]

[1] Worldwide, Cyberattacks are On The Rise," Information Age, Nick Ismail, March 26th, 2019
[2] "Digital Business Requires Cyber Security," Gartner, 2019

CHAPTER 1

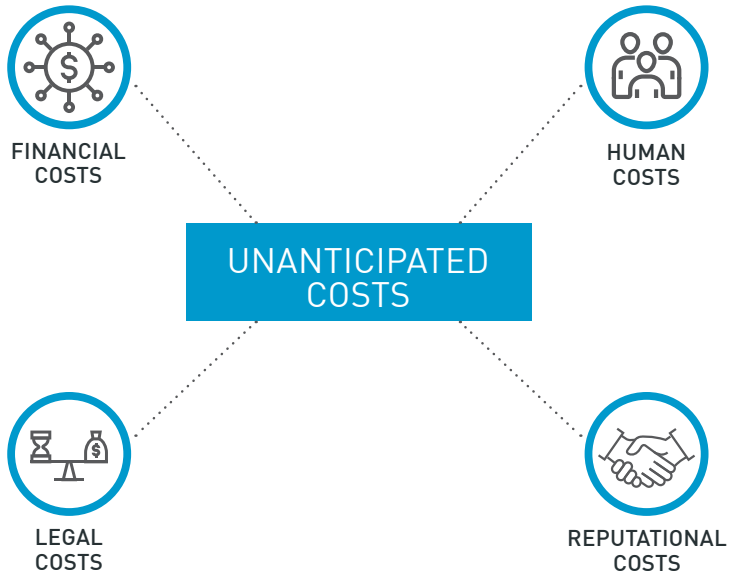
SMBS AND EXTREME DAMAGE FROM DATA BREACHES

In 2018, the average cost of a data breach forced organizations to spend $3.86 million USD per incident[3].

After intensive effort, you've mastered your market, earned your customer's patronage, hired the best talent, conducted a successful digital transformation, and developed a stable business. On top of that, your organization has made a meaningful contribution to society. Those 60-80 hour work weeks have finally paid off, and you're seeing the dividends. It would be tragic if everything that you've worked towards were suddenly demolished. Unfortunately, the reality of a downfall is closer than you might like to think.

As a decision maker, you may already know that 50% of businesses in the United States fold after five years, and 60% of U.S.-based SMBs that get hit with a cyber security attack fail within six months.[4,5] While some businesses can survive a cyberattack, the ramifications can be devastating, and often result in unnecessary losses.

When faced with a damaging cyber incident, businesses can expect to encounter sky-high unanticipated costs, ranging from financial loss, to productivity disruptions, to legal expenditures, to remediation efforts.



[3] "The Average Cost of a Data Breach," Security Today, Sydny Shepard, July 17th 2018
[4] "Why small businesses fail infographic," Business Insider, Jeff Desjardins, August 2nd, 2017
[5] "60% of Hacked Small Businesses Fail. How Reliable Is That Stat?," Bank info Security, Eric Chabrow, May 3rd 2017

FINANCIAL COSTS

Six months or more can lapse before organizations uncover a breach. Unrecognized breaches can quietly decimate systems and escalate clean-up costs. When breaches are recognized within 30 days, companies save as much as $1 million in remediation and restoration fees.[6,7] Having an incident response team can also help reduce costs.

With rapid counteractions from incident response teams, costs drop from $148.00 per compromised record to $135.00 per compromised record[8]. However, if an organization experienced the loss of 30,000 records, at a cost of $135.00 per piece, that would still cost the organization roughly $4 million in expenses. A breach of a million records, at $135.00 per record, would cost a company $1.3 billion.

According to the Ponemon Institute, the average cost of installing automated cyber security is only $2.8 million, making it significantly more cost effective to purchase quality cyber security than to risk the potential for a breach.[9]

The probability of experiencing a data breach of at least 10,000 records is 27.9%. In contrast, the chances of a person contracting the flu ranges from 5-20%.[10]

HUMAN COSTS

Is it more likely that your organization will get hit with a data breach, or that you will come down with the flu? The answer is a data breach. The probability of experiencing a data breach of at least 10,000 records is 27.9%. In contrast, the chances of a person contracting the flu ranges from 5-20%.[10]

When a data breach disrupts the daily routine, your IT workers are redirected from current projects to conduct damage control. Given that networks are often taken offline during the investigation process, non-IT workers may be unable to continue with job duties at all. Staff may also wonder if the organization will slash jobs to recoup attack expenses.

---

[6] "Survey Finds Breach Discovery Takes an Average 197 Days", Security Boulevard, Michael Vizard, July 18th, 2018
[7] "2017 Cost of Cyber Crime Study," Ponemon Institute, 2017
[8] The Average Cost of a Data Breach," Security Today, Sydny Shepard, July 17th 2018
[9] "2017 Cost of Cyber Crime Study," Ponemon Institute, 2017
[10] "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT", Security Intelligence, Larry Ponemon, July 11th, 2018

People often vote with their feet. They will walk away if they feel that they cannot trust you.

LEGAL COSTS

In the United States, the Federal Trade Commission (FTC) can charge organizations with violating Section 5 of the FTC Act, which fines organizations for careless business practices, and deceptive behaviors.[11] Fifty-two different cyber security-related bills across individual states also aim to protect consumers and to assign penalties to organizations for negligent security practices.[12] Broader federal mandates and penalties are still under development within the US, but you can expect to see them soon.

The United Kingdom is well on its way in this regard. In the UK, legislation now requires that companies guilty of inadequate data protection pay a penalty of up to €20 million euros, or 4% of global turnover, depending on the greater number.[13] The data privacy laws in Europe are written into a compendium of 11 chapters and 99 articles.[14]

Brazil is set to implement data protection laws similar to those of Europe. The *Lei Geral de Proteção de Dados Pessoais* (LGPD) will go into effect in August of 2020. As with GDPR, LGPD retains extraterritorial impact, and corresponding legal penalties.[15]

Other countries from Bahrain to Bosnia and Herzegovina to Israel to Switzerland are either amending current data privacy legislation, or introducing new legislation.[16] These policies are likely to include fines for evading, or inadequately attending to the restrictions.

REPUTATIONAL COSTS

Finally, reputational damage leaves a permanent scar on an organization's image. Conscientious consumers may cease to conduct business with an organization that appears to have inadequate cyber safeguards.

Having a pristine reputation is an intangible, but immensely valuable asset. It gives clients confidence in working with you.

Upon experiencing a cyberattack, ensure that the PR team works to maintain the company's public image, and that senior leaders begin new initiatives to retain or regain consumer trust, as needed.[17]

---

[11] "Protecting Consumer Privacy and Security", Federal Trade Commission
[12] "Cybersecurity Legislation 2018", National Conference of State Legislators, February 2nd, 2019
[13] Ibid
[14] GDPR vs Australian Data Privacy Regulations: 5 Key Differences", Information Age, Nick Ismail, March 5th, 2018
[15] "Brazil's New Privacy Law One Year Away," National Law Review, Sheppard Mullin Richter & Hampton, August 21st, 2019
[16] "Data privacy law," DLA Piper, February 25th, 2019
[17] "Total Cost of a Data Breach- Including Lost Business- Keeps Growing", NBC News, Herb Weisbaum, July 30th, 2018

CHAPTER 2

TYPES OF CYBERATTACKS

Cyberattacks manifest and disrupt enterprises in different ways depending on the mode of attack. The most common types of attacks make use of phishing, malware, bots, DDoS and data exposure. Within these broader categories, well-known sub-categories exist, with some of these even maturing into household names.

- PHISHING: Phishing can take a variety of different forms, but the common thread is that a person with malicious intent deliberately convinces an unsuspecting individual to divulge sensitive personal information.[18] Phishing scams can consist of fraudulently sent emails asking for donations, emails enticing users with prizes, or emails containing malicious links. The FBI has suggested that the cost to US businesses in regards to phishing may be as high as $5 billion annually.[19]

- MALWARE: This is an umbrella term for multiple different types of attacks that attempt to intrude on machines. Common types of malware include ransomware, worms, Trojans, rootkits, adware, and spyware. To advance your understanding of what's at stake, simple definitions are below:

  RANSOMWARE: This strain of malware can hold computer systems, files, documents and databases hostage though encryption. The hackers deploying the ransomware ask for a ransom. A deadline is assigned for the ransom payment, and if the deadline passes, the ransom demand doubles or files are permanently locked. Should your network incur an infection, it is never recommended to pay the ransom. This only encourages the practice.

  WORMS: Computer programs that can run independently, and can propagate complete working versions of themselves, either within an already infected system, or within a new system.

  TROJAN: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function.

  ROOTKITS: A rootkit is a type of malware designed to burrow deep into your computer, avoiding detection by security programs and users.

[18] "These are the Most Common Types of Phishing Emails Reaching your Inbox", ZDNet, Danny Palmer, July 23rd, 2019
[19] "What is Phishing? Everything You Need to Know to Protect Yourself from Scam Emails and more," ZDNet, Danny Palmer, September 6th, 2017

ADWARE: Adware on a compromised website can load malware onto your computer. Other than displaying advertisements and collecting data, these types of program generally do not make their presence in the system known: there will be no signs of the program in the system tray, and no indication in the program menu that files have been installed.

SPYWARE: Programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

BOTS: Using bots, hackers can infiltrate multiple internet-based devices, and then link them altogether. In doing so, the owner can control the devices remotely, using malware, without the knowledge of the device's owner.[20] The hacker's actions can create chaos, of either the electronic or physical variety.

DDOS: Distributed denial of service attacks (DDoS) attempt to disrupt service to a website, or an online platform.

DATA EXPOSURE: This type of breach occurs due to poorly secured or unsecured data assets.

Cyberattacks are growing in sophistication and complexity. As visible from the array of attack options outlined above, cybercriminals are cunning, and relentless. Be sure that your organization implements advanced threat prevention, detection and testing strategies.

[20] "On the Way to a Safe and Secure Smart Home," ScienceDaily, Fraunhofer-Gesellschaft, September 3rd, 2014

CHAPTER 3

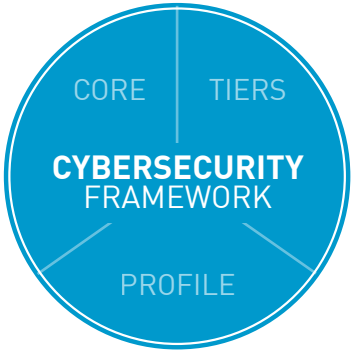
FINDING THE RIGHT PROTECTION

"...massive institutional breaches don't need to happen as often as they do. Many occur not because of complex and sophisticated hacking, but because organizations have made basic and potentially avoidable mistakes in implementing their security schemes"*

Choosing the right security product or products and creating a balanced security portfolio can seem like a never-ending process and a losing proposition. However, you can stay safe with the right planning and tools.[21]

To help you find the best possible security for your organization, the US National Institute of Standards in Technology (NIST) has published a clear framework for owning and managing cyber risk.

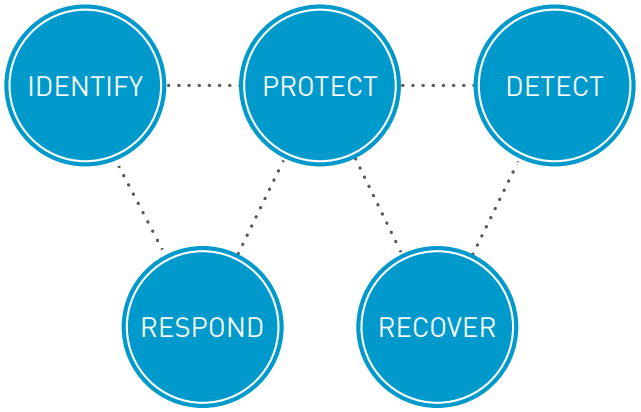
The framework consists of three primary focal points:



1. IMPLEMENTATION TIERS: The framework's implementation tiers guide business leaders in assessing the rigidity of their organization's security posture, and in determining whether goals and fiscal decisions align with the current levels of cyber risk.

* "Wired Guide to Data Breaches," Wired, Lily Newman, December 7th, 2018
[21] "the WIRED Guide to Data Breaches," Wired, Lily Newman, December 8th, 2018
[22] "An Introduction to the Components of the Framework," NIST, August 10th, 2018
[23] "New to Framework," NIST, April 23rd, 2019

2. A FRAMEWORK CORE: The framework core consists of five broad functions:



Within each core function there are categories and, sub-categories that point to more specific elements to consider.

"There are 108 Subcategories, which are outcome-driven statements that provide considerations for creating or improving a cyber security program," writes NIST.[22]

Specific information about the subcategories can be found here.

3. A PROFILE: Create a profile of your organization to gain a deeper sense of the current operating state of the organization as compared to organizational objectives and risk appetite, among other factors. Organizations are encouraged to outline a "current" profile, and to develop a "target" profile to work towards. To learn more about NIST's framework and companion roadmap, click here.

In addition to the NIST framework, basic considerations that organizations should examine prior to selecting a security product or products include: Top-notch visibility, a customized dashboard, and scalable, comprehensive architecture.[23]

[22] "An Introduction to the Components of the Framework," NIST, August 10th, 2018
[23] "New to Framework," NIST, April 23rd, 2019

VISIBILITY

Ensure that your architecture includes powerful visibility into your network. With limited visibility, how can you monitor which pieces of your system are operating optimally, and also see where your weak points lie? How can you use data to make informed business decisions about defense?

After Desert Research Institute (DRI) chose a Check Point security solution, senior network engineer, Ryan Coots, reported that the company gained full visibility through the architecture, making security straightforward, and efficient.

Monitoring data and reporting logs through a single pane of glass permits teams to quickly identify and analyze threats and to rapidly implement policies or measures to provide active defense. Companies can easily get to the bottom of user complaints- whether it's a lethargic network, or a potential cyber incident. With enhanced visibility, organizations can obtain instant insights into user traffic trends, resource consumption, and supplemental indicators of network performance, allowing them to quickly zero in on any threats.[24]

"You've got to track your security portfolio performance regularly to see which investments are delivering. Just as with your financial portfolio - measuring the performance of the [security] portfolio regularly is important."[25] Without adequate visibility, it is impossible to see your current security posture.

In seeking maximum visibility, be sure to choose a solution that's fully customizable.

CUSTOMIZABLE CAPABILITIES

Get architecture with a range of customizable capabilities. Your business is unique, and the breadth and depth of security architecture necessary to protect it may change over time. With a customizable solution, your security configuration can change and adapt in conjunction with the business. No need to draw up a new budget, and reevaluate products. A customizable dashboard and controls support non-stop growth.[26]

SCALABLE, COMPREHENSIVE ARCHITECTURE:

To protect against the bulk of cyberattacks, and to maintain data integrity as your business continues to expand, select a scalable security solution that covers cloud, mobile, endpoints and IOT.

The importance of balanced, comprehensive cyber security cannot be overstated. When it comes to good cyber security, avoid leaving anything to chance.[27,28,29,30,31]

---

[24] "Desert Research Institute Elevates Data Security in a Dynamic Threat Ecosystem with Check Point", Check Point Software Technologies
[25] "How to Select The Right Products For Your Cybersecurity Portfolio," Forbes, Dan Woods, April 3rd, 2017
[26] "How to Build Secure Networks that are Both Agile and Customizable", NetworkComputing, Ray Watson, August 1st, 2019
[27] "Cloud and Mobile Deployments Are the Weakest Links in Enterprise Networks, shows Check Point's 2019 Security Report," GlobalNewsWire, February 20th, 2019
[28] "As IoT Attacks Increase 600% in one Year, Businesses Need to up Their Security," TechRepublic, Alison Rayome, March 21st, 2018
[29] "Introducing SandBlast Mobile," Check Point Software Technologies, April 21st, 2017
[30] As IoT Attacks Increase 600% in one Year, Businesses Need to up Their Security," TechRepublic, Alison Rayome, March 21st, 2018
[31] "DDoS Attacks Evolve To Conscript Devices Onto The IoT," Forbes, Russ Branham, February 4th, 2018

" Many companies rely on basic mobile policies using mobile device management (MDM) or enterprise mobility management (EMM) solutions. While these can be helpful, they are unable to detect the most recently created malware or new vulnerabilities in networks, operating systems, and apps."

- CP Security Guide for Executives

AT A GLANCE

18% of organizations experienced a cloud security incident during the past year, and over 90% of organizations report concerns in regards to their cloud security.

Every company is under mobile attack. A survey by Check Point researchers revealed **89%** experienced at least one Man-in-the-Middle attack over a wi-fi network.

In 2018, a Ponemon Institute study found that **two thirds** of enterprise players had been compromised by attacks on endpoints.

The rush to put loT devices on the market meant that manufacturers didn't initially think much about the products' security. From 2016-2017, loT threats increased by **600%**.

Hackers often use loT for DDoS attacks. According to the Ponemon Institute, DDoS attacks costs companies an average of **$1.7 million** in a combination of lost profits and clean-up.

CHAPTER 4

ENGINEERING YOUR INCIDENT RESPONSE (IR) PLAN

"By failing to prepare, you prepare to fail"
–Benjamin Franklin

77% of organizations lack an incident response (IR) plan[32]. An IR plan is a must when it comes to preparing for a cyberattack, offering a blueprint for how to proceeded when the hackers do get in.

A good IR plan indicates a clear chain of command in the event of a cyber emergency, and lays out individual steps that should be taken to minimize an incident's impact.

The plan should not only list the IT team as the primary line of defense, it should also involve the legal team, HR and PR departments.

- From a legal standpoint, a general council can provide information pertaining to liability, and can advise the company in taking legal action against a vendor or a customer, if necessary.
- The HR team is suited to handling the relationship with the employee/s who may have been involved in the threat.
- The PR team can position itself to manage media impressions of the incident.[33]

Conduct a business analysis, and structure your IR plan around the information gathered. This will ensure that your plan complements business operations and objectives.

Additional best practices for developing an IR plan can be found within the NIST framework.

Be sure to test your plan ahead of an actual breach. Over 50% of organizations fail to regularly test their IR plans, pitching organizations into a frenzy when it comes to handling an actual cyber incident.

[32] "77% of Businesses Lack Proper Incident Response Plans," Dark Reading, March 14th, 2018
[33] "Building Your Incident Response Team: Key Roles and Responsibilities," DataInsider, Tim Bandos, July 27th, 2017

CYBER INSURANCE

Cyber insurance is neither an incident response plan, nor a substitute for a strong cyber resilience profile. Cyber insurance is a fail-safe.

Nothing can compare with a robust security architecture.

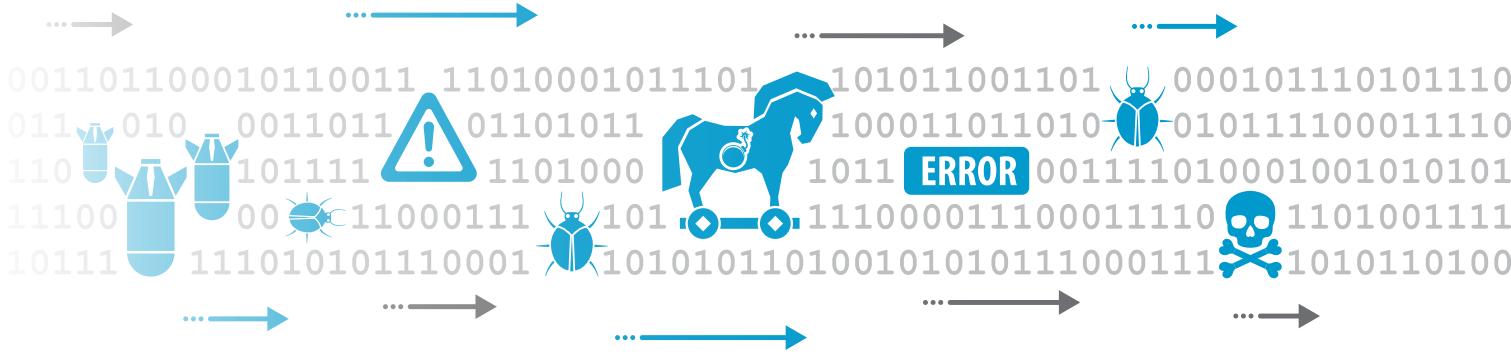
But if you're going to explore the option...

Two types of cyber liability coverage exist: 'first-party' and 'third-party'. First-party coverage offers reimbursements for direct losses that affect an organization or an individual. 'Third-party' cyber coverage takes care of claims and legal actions thrown at an organization by its customers or partners.

When buying a policy, be sure to know exactly what it does and does not cover. Say 'no' to a policy that uses vague, non-committal language. For example, if the policy notes that it will reject coverage for "[your] failure to maintain or take reasonable steps to maintain security," steer clear. In legal exchanges, the person defining 'reasonable' undoubtedly will not be the buyer.

Cyber insurance is popular, and is due to reach an estimated market value of $7.5 billion by 2020.[34] However, some analysts question whether cyber insurance will continue to exist in the long-term, as an increasing number of cyberattacks force insurance companies to pay-up.[35]

If you would like assistance in determining what type of insurance is right for your organization, visit this cyber insurance buyer's guide.[36]



[34] Ibid
[35] Ibid
* "Digital Business Requires Cybersecurity", Gartner
[36] Ibid

CHAPTER 5

ARE YOU REALLY OUTSMARTING THE HACKERS?

In building the foundations for success, ensure that your organization considers the following techniques as you move forward.

1. Of course, increasing employee awareness of threats is likely the easiest and most obvious means of building a more resilient organization. When employees know what to keep an eye out for, they are less likely to precipitate an incident. Offer formal trainings, and ensure that managers are available to answer questions on an ongoing basis.

2. Open source and commercial security testing tools are available online, and the more variety that you can deploy, the better your security will become.

   Organizations also frequently choose to conduct red teaming exercises, where a team of IT professionals tries to identify weak spots in servers, endpoints, wireless networks, software applications and physical points of entry. If red team members can hack into a system, that cues a company to invest in additional cyber security measures.

"The thing that kept me awake at night [as a NATO military commander] was cyber security. Cyber security proceeds from the highest levels of our national interest...through our medical, our educational to our personal finance [systems]"

-Admiral James Stavridis,
Ret. Former NATO commander*

3. Adopt a comprehensive threat prevention architecture that can secure all of your systems, from endpoints, to networks, to mobile devices to IOT. This is your best bet for defending your organization. Rather than implementing point-solutions to take care of these different points of entry, you can purchase a single consolidated security solution. In addition to offering ease of use, consolidated architectures can also reduce operational overhead, and the total cost of ownership. Win-win! Read more about comprehensive solutions by clicking here.

4. Ensure that your architecture includes strong firewalls. Firewalls enable segmentation, and can authenticate traffic as it enters and exits your network. Modern firewalls offer advanced network protection, with features like anti-bot technology, anti-virus, identity awareness, application control, anti-spam, a VPN and more.[37]

5. Obtain a virtual LAN. This tool can improve overall network function and help direct traffic by providing additional network compartmentalization and segmentation. The virtual LAN can determine which devices can or cannot "talk" to one another, thereby reducing the potential for an attack to spread.

6. Install a VPN (virtual private network). Installing a VPN is a means of ensuring privacy within your internet connection. Your data, and your employee's data travels through what is effectively a 'tube' to a server. The contents of that tube cannot be made visible to prying eyes on the network[38]. Due to the technical configurations of VPNs, owners can obtain granular levels of information, and can deploy tight access control, even for remote workers.[39]

7. Close 'backdoors' to privileges. Backdoors refer to unsecured points of entry for hackers. When able to access a network from a backdoor, an attacker can potentially deploy spyware, ransomware, a DDoS attack, or other malicious applications. To protect backdoors, change your default passwords, monitor network activity, and choose applications and plug-ins with care.[40] In addition, use a good cyber security solution.

8. Implement Role-Based Access Control. This can be used to improve visibility, and to enhance control over corporate resource.[41] Solutions like the Identity Awareness Software Blade help companies gain granular insights, automatically enforce policies, and prevent unauthorized access.

[37] "Next Generation Firewall," Check Point Software Technologies
[38] "What Is a VPN, and Why You Need One," PCMag, Max Eddy, August 26th, 2019
[39] "How to protect the network from the inside out," ComputerWorld, Atul Bhatnagar, May 13th, 2004
[40] "Backdoor," Malwarebytes
[41] "Identity Awareness Software Blade," Check Point Software Technologies

IN CONCLUSION

Security often feels like an ongoing cat and mouse game, with hackers continually bating organizations and organizations scurrying to find new ways to halt the attackers. However, with awareness, the right mentality, an incident response plan, and a resilient posture, you can minimize your organization's risk of a cyber threat.

To stay up-to-date on cyber threats and industry insights, integrate readership of CyberTalk.org to your daily routine. This is the internet's best daily cache for cyber news, trends and more. Subscribe to the weekly newsletter to have the finest cyber news delivered straight to your inbox.

For more on the best comprehensive threat prevention strategies, read this report.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com