A CYBERSECURITY FIELD GUIDE FOR EXECUTIVES:

Putting the Cyber Landscape in Perspective

Check Point®
SOFTWARE TECHNOLOGIES LTD

Introduction

We've come a long way from the days when cybersecurity—if it was even on the radar—was the job of the IT Director. Today, there is consensus that not only does it need to be a top priority for organizations, but that executives at the highest levels, including boards of directors must be accountable.

Yet, oddly enough, a recent study[1] by Frost & Sullivan reports that one-third of executives from major businesses don't see the value of data security. Worse, those same leaders work at companies that had suffered data breaches and were aware of the significant impact to the company's bottom line. The report found that businesses that suffered major data breaches ended up losing half their customers. We appear to have reached a tipping point, where cybersecurity will drive customer loyalty and competitive differentiation. The sooner business leaders become aware of that, the stronger their organizations will be.

With massive cyberattacks worldwide and new laws—such as the European Union's (EU) General Data Protection Regulation (GDPR), the lesser known EU Network and Information Security Directive (NISD) specific to critical infrastructure organizations, and the more recent California Data Privacy Law—protecting sensitive data, intellectual property, and network operations has become not just essential but mandatory. This guide will walk you through the key areas to focus on and the actions to take to secure your organization.

1. Frost & Sullivan White Paper, "*The Global State of Online Digital Trust*," 2018.

WHY YOU NEED TO CARE: THINGS CHANGE

With all the daily blasts of news about cyber attacks, it can be easy to fall victim to cyber fatigue—and lose sight of where your organization sits in the scheme of things. Could your company be a target? How might hackers attack you? What would be the motivation for a cyber attack on your organization?

More importantly: Is your business prepared to withstand a cyber attack? Would you even know if you **had** been breached?

Check Point research shows that cyber attacks are not only *not* going away—they're evolving and finding new ways to infect. While many companies might have security infrastructure in place, a Check Point survey of IT professionals shows that 97 percent are using outdated cybersecurity technologies.

At issue is that when organizations first began to focus on cybersecurity, it was all about securing the network perimeter. But as business extended to mobile and remote ways of working—and then to the cloud—security became an afterthought, if it was considered at all.

In fact, half of all security incidents handled by Check Point's Incident Response team in 2017 were cloud related. Not only that, all businesses have had some kind of mobile cyberattack. It doesn't help when the convergence of BYOD and IoT collide and fake apps abound in mobile apps stores. In the past year, Check Point discovered that more than 300 apps in the Google Play Store had malware and were downloaded by more than 106 million users.

The reality is that as technology has evolved to spark new innovations and help companies break into new markets, the hackers have followed suit.

With each new advancement in cyber security protections, two factors have come into play:

1. Cyber criminals have invented new ways to deliver payloads and have even tapped unexpected channels (fax machines, snail mail with CDs). Plus, with the leaking of the NSA hacking tools in 2017, even amateurs can launch cyber attacks like a pro. And if they can't, they can easily find someone who can do it for them, as an entire industry has sprung up on the Dark Web, to support and perpetuate the hacking industry.

2. As companies have evolved their security, they've done it by adding on what they have seen as the latest and greatest point products, versus taking a big-picture approach. As a result, they find themselves with a collection of disparate solutions that don't integrate in a cohesive way, leaving portions of their infrastructure exposed. Layer in the complexity of working with third-party vendors who have their own security challenges, and you have a situation that's ripe for attack.

To see this more plainly, take a look at how the cyber landscape has evolved.

The late '80s, Generation I: Hackers were typically pranksters. Virus attacks on stand-alone PCs began mostly as annoyances or mistakes. To halt disruption, anti-virus products were developed.

The mid-'90s, Generation II: As the internet started to become central to business and our lives, hackers began to organize and communicate among themselves, laying the groundwork for cyber crime for financial gain. Malicious and volatile software began to crop up. This gave rise to the first firewall, along with intrusion detection systems (IDS)—emphasis on detection.

The early 2000s, Generation III: Attackers began to analyze networks and software to find and exploit vulnerabilities throughout the IT infrastructure. Firewalls, anti-virus, and IDS products were proving to be insufficient in the face of exploits. This sparked the era of a hodge podge of products and patchwork security models as businesses scrambled to protect themselves. Check Point began shifting its focus to lean less on detection and more on prevention and launched intrusion prevention systems (IPS) products.

Then, things *really* began to change.

Around 2010, Generation IV: Cyberattacks reached a new level of sophistication, ranging from international espionage to massive breaches of personal information to large-scale internet disruption. Attacks were hidden in everything from resumes to picture files—evasive and polymorphic. While internet security of the 2nd and 3rd generations provided access control and inspected all traffic, it couldn't validate actual end-user content received in email, such as file downloads of photos or PDFs. In response, Check Point introduced anti-bot and sandboxing products to address previously unknown and zero-day attacks.

Around 2017, Generation V: Advanced 'weapons-grade hacking tools were leaked, giving attackers massive scale. Now they could move fast and infect large numbers of businesses and entities across huge swaths of geographic regions.

These large-scale, multi-vector mega attacks that we now see happening on a regular basis spark a need for integrated and unified security structures. Prior generations of patchwork technologies, which focus on detection, are proving to be no match for the rapid and stealthy attacks of the fifth generation.

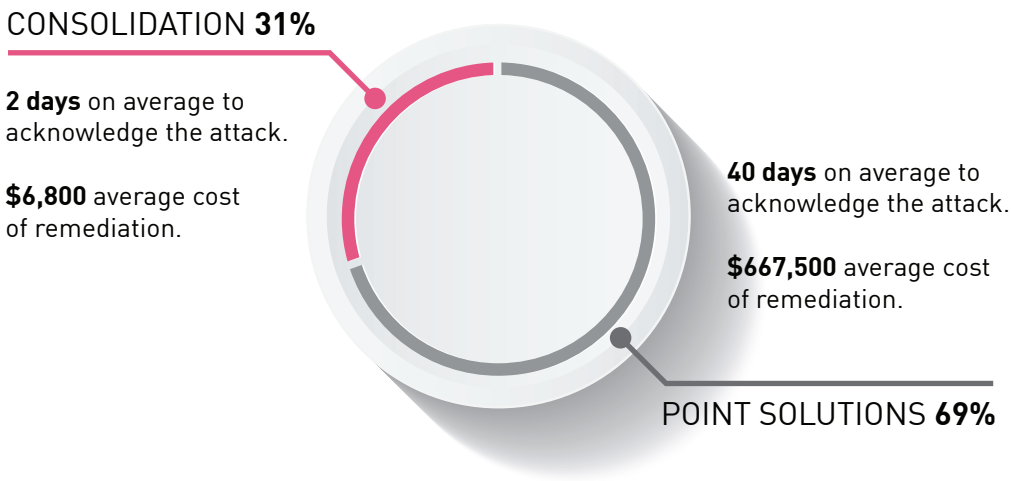
To remain viable in the face of today's threats, organizations need to shift from detection to prevention. Unified architecture with advanced threat prevention solutions help organizations take advantage of threat intelligence in real time, preventing attacks on virtual instances, cloud deployments, endpoints, remote offices, and mobile devices.

Businesses that subscribe to the adage "adapt or die" will not only be more secure, they'll be much better positioned from a competitive standpoint because they'll be able to operate more nimbly. Those that hang onto legacy technology are playing a dangerous game of risk.

How to view the modern cyber security infrastructure

To withstand the type of advanced generation attacks that we see today, organizations need to rethink their overall approach. It comes down to integrated architecture versus discrete products. Not only is it easier to manage, it can deliver dramatic cost efficiencies. As the illustration below shows, a consolidated security infrastructure helps organizations identify cyberattacks markedly faster, leading to a cost savings of hundreds of thousands of dollars.

POINT SOLUTIONS vs CONSOLIDATION



What is 5th-Generation Security?

Given the complexity and sophistication of the latest generation of attacks, businesses need to not just take a different approach, but also adopt specific technologies.

In a nutshell, it's prevention-based security that spans networks, cloud, mobile, and endpoints. It consolidates the entire IT infrastructure for centralized management.

5th-generation security goes beyond the previous generation of security to provide key advantages:

- Consolidates next-generation-firewall (NGFW), sandbox, bot security, endpoint security, and other security controls into a single security system.
- Shares real time threat information throughout the system.
- Takes advantage of API-based security to automate system management and threat remediation—especially critical when ransomware attacks strike.
- Boosts visibility for insights into all activity across all devices.
- Uniformly prevents attacks across a business's entire IT infrastructure of computer networks, virtual instances, cloud deployments, endpoints, remote offices, and mobile devices.

Check your assumptions

With technology changing so fast, security can sometimes seem like a goal post that is continually moving. Below are corrections to some of the more common misperceptions.

1. IF I HAVE SECURITY ON PREMISES, I DON'T NEED TO SECURE THE CLOUD

This is a dangerous assumption that can wreak havoc with safeguarding your organization. Cloud security is just as necessary as your other security. With more and more workloads moving to the cloud and employees storing files and using apps in the cloud, sensitive data risks greater exposure. Without the right technologies in place, IT has less control and less visibility. Not only that, dozens of high-profile data breaches have been the result of unsecured cloud deployments. The lesson: If you're working with a cloud provider—or just a third-party vendor, security is a shared responsibility. Don't take for granted that security will just magically be put in place.

2. AS LONG AS I MEET COMPLIANCE REQUIREMENTS, MY ORGANIZATION IS SECURE ENOUGH

What many don't realize is that security regulations are typically tied to very specific situations and are not as comprehensive as true security needs to be. If your protections are limited to what is required to comply with regulations, you are merely covering the basics. This can be a very expensive mistake considering the cost of remediation, brand tarnish, and loss of sensitive information and intellectual property.

3. TIGHT SECURITY TAMPS DOWN PRODUCTIVITY AND LIMITS INNOVATION

In fact, good security enables just the opposite. When the right protections are in place, your business can take advantage of emerging technologies to spur greater agility. Plus, your employees can securely collaborate more freely—with greater confidence.

4. MOBILE ISN'T A BIG PROBLEM

This is another myth that can lead to an insecure organization. The reality is that hackers have turned to mobile as the great, untapped frontier. From zeroing in on vulnerabilities in mobile apps to infecting with malware specifically designed for mobile devices, cyberattackers have changed the mobile security landscape. Check Point's Mobile Threat Research Team found that every organization had suffered a mobile malware attack in the past year. Not only that, 89 percent experienced at least one man-in-the-middle attack over a WiFi network. All of this is sobering, given that it takes only one compromised device to penetrate your security perimeter.

5. MDM IS ENOUGH

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. Security infrastructure for corporate PCs and laptops isn't enough either, since mobile devices work beyond the network, creating potential security issues and enabling malware to enter.

6. SECURE CONTAINERS ARE SAFE

Secure containers for data management platforms provide security *inside* the enterprise perimeter. However, mobile devices often access systems and apps like Salesforce, Oracle, or SAP *outside* the perimeter. As a result, this risks exposure to network spoofs or man-in-the-middle attacks, which can eavesdrop, intercept, and alter traffic. Everything a user does, including entering passwords, could be intercepted by criminals and used to breach the perimeter.

7. IOS IS IMMUNE

Contrary to popular belief, Apple's iOS is not immune to threats. Some organizations using MDMs unwittingly distribute infected apps to iPhones and iPads. Apps from unauthorized, unreliable app stores can also harbor viruses; hackers have even compromised Apple's development tools, sneaking malware into new apps without the developers' knowledge.

8. MOBILE ANTIVIRUS IS ALL I NEED

It's unfortunate that the same advanced detection techniques used on PCs and laptops can't extend to mobile devices. That's because devices used on-the-go have limited performance and battery life. Add to that, mobile antivirus solutions are limited compared to PCs. They can uncover malicious code in apps by looking for unique binary signatures that identify known malware. But, criminals can still get through: just a slight change in the code, such as adding a simple line that does nothing, generates a new version of the malicious app, which lets it slip by undetected by the antivirus program. So, while you might be protected against known viruses, a new one might hit your device before an antidote has been developed.

9. EXECUTIVES AT THE TOP LEVEL DON'T NEED EXTRA PROTECTION.

Nothing could be farther from the truth. The c-suite, especially, is considered a high-value target because of their access to corporate assets and sensitive information.
Spearphishing and spoofing attacks are common, attempting to trick busy executives into forwarding financial information or other sensitive data. Also, executives often keep that confidential information on their devices for quick and easy access, not always conforming to security best practices. Keeping devices and apps updated and ensuring proper access restrictions is critical. Not to mention educating and reminding everyone that phishing attacks have become far more successful due to social engineering tactics.

Types of threats

The range of threats is vast. And their names are not, necessarily, easily intuited. Below is a review of some of the more common cyber concerns.

Bots: Like worms or Trojans, bots spread once inside a network. Where they differ is that they communicate back to a command and control (C&C) machine and receive instructions for automated activities. This lets hackers easily orchestrate spam campaigns or DDoS attacks. Check Point researchers found that bots try to communicate with C&C more than 1,630 times per day, or every 53 seconds. Almost 75 percent of organizations studied were infected with bots in 2015. Worse, 44 percent of those were active for more than four weeks.

Cryptojacking: A type of cyber attack where the victim's systems and processing power are taken over by a hacker in order to mine for cryptocurrency.

Data Loss/Data Exfiltration: The loss of data that is transferred from the target victim either manually with a USB device or through malware designed to pull critical information.

DDoS (Distributed Denial of Service): A type of malware that utilizes multiple resources to overwhelm and hog bandwidth so a website or network hangs or crashes entirely.

High-Risk Applications: Programs that individuals bring into the workplace, which they rely on for their own purposes, even though unsanctioned by IT. Some of these are considered high risk because of the number of vulnerabilities found and the potential for exposure to cyberthreats. File sharing, remote admin, and anonymizers are especially risky.

Known Malware: Malware that has previously been identified and has a signature associated with it. Because many security tools analyze traffic based on an ever-growing library of signatures, known malware is easy to spot if your subscriptions are up to date.

Ransomware: Malware that prevents access to files or computer systems until a sum of money is paid.

Spear Phishing: A type of attack that uses email to pretend to be from an individual or business that you know, in order to obtain sensitive information; trick you into clicking on a malicious link or attachment; or to prompt you to unwittingly perform an action designed to benefit the perpetrator. Phishing that is conducted via short message service (SMS) texts is called SMS Phishing.

Spyware: Software that is designed to allow surveillance by spying on a user's online activities, which can include emails, photos, videos, texts, and other forms of communication.

Trojans: Malware that relies on social engineering or some kind of disguise so that it makes users think it is a legitimate program to load or execute.

Unknown Malware: New, malicious software that has not yet been identified and does not yet have a signature. By just changing the code of known malware slightly, you can easily create new, unknown malware.

Viruses: Malware that integrates into a program and spreads. It is reliant on someone opening or running the program that hosts the virus.

Worms: Like viruses, worms, too, can self-replicate. They differ from viruses, though, by not requiring a host program. They get in through social engineering or are activated through exploited vulnerabilities on target systems.

Zero-Day Malware: Malware that is designed specifically to attack vulnerabilities that either haven't yet been identified or that don't yet have patches.

Ask questions

Begin by asking the right questions. Below are 10, which are adapted from questions provided by both Homeland Security[2] and CSO.com[3].

1. What is our reporting policy and how frequently is executive leadership kept informed?
2. When was the last time we had a security risk assessment? How did we score? What's been done to address the findings?
3. Is there anything in particular that makes us more of a target for cybercriminals?
4. What does an average week look like in terms of volume and types of incidents?
5. How frequently do we conduct a data inventory?
6. How is our data categorized and classified for access?
7. What security controls are in place to protect our data assets?
8. Do we have an incident response plan?
9. Do our employees receive security training?
10. What is the lifecycle of our software and hardware?

[2] David Higgins, CSO.com "*10 Things Every CEO Should Ask About Security in their Organization.*"
[3] Homeland Security, "*Cybersecurity Questions for CEOs.*"

Focus on prevention—it's cheaper than the alternative

Cover the Basics

With threats growing and constantly evolving, it's critical to combine multiple methods of protection, detection, and defense to stay ahead of the cybercriminals.

For starters, make sure your organization is vigilant about applying software patches. Implement updates as soon as vendors release them. Despite the fact that vulnerabilities exist in most software, surprisingly, many organizations don't take this seriously. As a result, hackers are able to get in by taking advantage with malware that zeroes in on these known vulnerabilities. Case in point: WannaCry could have been prevented had organizations updated their systems with the patch that had been issued a month or two prior.

In addition, don't forget about virtual patching: a temporary quick-fix security policy. Using an intrusion protection system, virtual patching safeguards against zero-day exploits and discovered vulnerabilities that do not yet have a patch.

Use the Right Technologies

Think about your network—on premises and in the cloud—as you would any structure that you need to stabilize and safeguard. You build in layers of reinforcement to ensure it will be able to withstand potential issues. Similarly, with your network, you want to make sure you have multiple layers that can coordinate and reinforce a range of protections—to keep threats out; keep confidential data in; and be able to identify the right people with the right permissions. All while preventing spam, keeping email secure, and preventing your employees from being lured to high-risk websites.

Think in terms of architecture, versus point products. Just like you want a house that is wholly integrated and not cobbled together, leaving gaps, your IT infrastructure should be the same.

Look for solutions that:

- Focus on prevention versus merely detection
- Investigate all incoming file types
- Identify zero-day threats within and beyond the operating system
- Have the highest catch rate
- Include deep OS- and CPU-level sandbox capabilities to detect and block malware; and threat extraction to reconstruct incoming documents
- Are integrated to automatically coordinate among different protections such as advanced threat prevention, security gateway, application control, antivirus, identity awareness, intrusion prevention, and URL filtering
- Protect across networks, mobile, cloud, and endpoints with centralized monitoring and management

Know How to Respond to Incidents —Timing is Everything

In the 2016 IBM Ponemon Data Breach Study, the average number of days it took to identify a breach was 201 days. In the 2018 study[4] just two years later, in the era of fifth-generation attacks, the average time to detect and contain a mega breach jumped to 365 days—nearly 100 days more than a smaller scale breach (266 days).

What makes the timeline so significant is that the longer it takes to detect and contain the incident, the more it costs to clean up. According to the report, companies that contained a breach in fewer than 30 days saved more than $1 million compared to those that took longer than 30 days.

Pushing days aside, the reality is that each second matters, as well. Attacks can spread quickly and leave a heap of damage in their wake. And, in the process, leave customers unable to follow through with purchases and employees unable to do their jobs.

At a minimum, Check Point recommends that your Incident Response Team be prepared to do the following, should a breach occur:

Assess. And alert the authorities! As quickly as possible, assess the situation, noting damage or loss, point of entry, time of breach, and any other details or characteristics you can identify. This information should be shared with all designated people in your overall security plan, including the board, and be updated at regular intervals. Be sure to notify the authorities as well. Don't assume that the attack was aimed only at your business. Law enforcement can triangulate incidents and help you get farther along in the investigation.

Contain. Next, contain the incident. From the immediate standpoint, that means isolating the segment of the network where the problem was spotted. If you're dealing with an attack that is being carried out by a bot through its command-and-control center, block the communication path.

Backup. Make sure your team conducts a full backup, to capture the environment at the point of attack, to help with forensics.

Secure. Prevent further damage by removing equipment or accounts that have been affected, but remember to keep them for forensics purposes; install patches and updates where necessary.

Validate. Before bringing your environment back online, be sure to test and validate that your system is clean and running as it should. If there is any unusual behavior, keep testing to identify the root cause.

Conclusion

Remember, everyone, ultimately, is responsible for the security of their organization. At the c-level, that responsibility is underscored. Make sure your organization has a plan—not just for how to build and manage a security infrastructure, but how to respond to and clean up after an attack. Those who look the other way—or don't tune in—are essentially neglecting their duty. Head in sand is not an option.

The biggest mistake you can make is to assume that you're done because you've already thrown resources at protecting your organization. Security is like a living organism. It has to adapt to the changing environment or it won't be effective.

To learn more about threats, the latest security technologies, or how an incident response team can help you, go to checkpoint.com.

[4] IBM, "*IBM & Ponemon Institute 2018 Cost of a Data Breach Study.*"

Test your network vulnerability with an instant assessment at **www.cpcheckme.com** and get a free personalized report.

CONTACT US

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
checkpoint.com