CYBER SECURITY WITH INTENTION

AN EXECUTIVE GUIDE

Check Point®
SOFTWARE TECHNOLOGIES LTD

WELCOME TO THE FUTURE OF CYBER SECURITY

INTRODUCTION

Whether you're in public or private sector, small business or enterprise, if you're in IT or an executive in your organization, it's incumbent on you to ensure that sensitive data, account information, intellectual property, and your network operations are protected. This guide will walk you through the key areas to focus on and the actions to take to secure your organization.

Every 81 seconds a known malware is downloaded. Think that's frequent? It's not, when you look at unknown malware: *That's* downloaded every four seconds. Let's face it. There's a good chance we're all at risk when even the United States Office of Personnel Management (OPM) can be breached—inadvertently leaking more than 21 million personnel records of government employees.[1]

Understanding the threat landscape can be hard enough. But overlay it with constantly changing compliance regulations and it becomes even more complex.

Today's business climate revolves around digital strategy, whether it's social media, e-commerce, demand generation, or all of the above. Add to that the increasing presence of artificial intelligence (AI) and IoT. When an organization has effective cyber protections in place, it is better able to take advantage of the internet and all aspects of the digital, connected experience. This helps spur engagement and innovation.

Businesses that subscribe to the adage "adapt or die" will be much better positioned from a competitive standpoint because they'll be able to operate more nimbly. It's hard enough when businesses hang onto legacy technology. But when they also shy away from taking advantage of technology that can protect them from current and emerging threats, it's like trying to chop ingredients with a dull knife: You can do it, but it's going to take longer and you could end up hurting yourself.

Remember: Ultimately, cyber protection is everyone's responsibility. For employees, it's up to them to handle sensitive data appropriately. For IT, it's up to them to understand network and device vulnerabilities and put protections in place. For executive and board leadership, it's up to them to oversee an organization's ability to withstand risk. Those who look the other way—or don't tune in—are essentially neglecting their duty. Head in sand is not an option.

[1] OPM Cybersecurity Resource Center. https://www.opm.gov/cybersecurity/cybersecurity-incidents/

FALSE SECURITY 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.

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 you are required to implement, 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, last year alone, at least one in five organizations experienced a mobile security breach. Of these, 39 percent downloaded mobile malware and 24 percent connected to a malicious Wi-Fi® network.[2] While testing mobile security for prospective customers, Check Point regularly finds five to 20 percent of enterprise devices are already compromised. A sobering fact, 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.

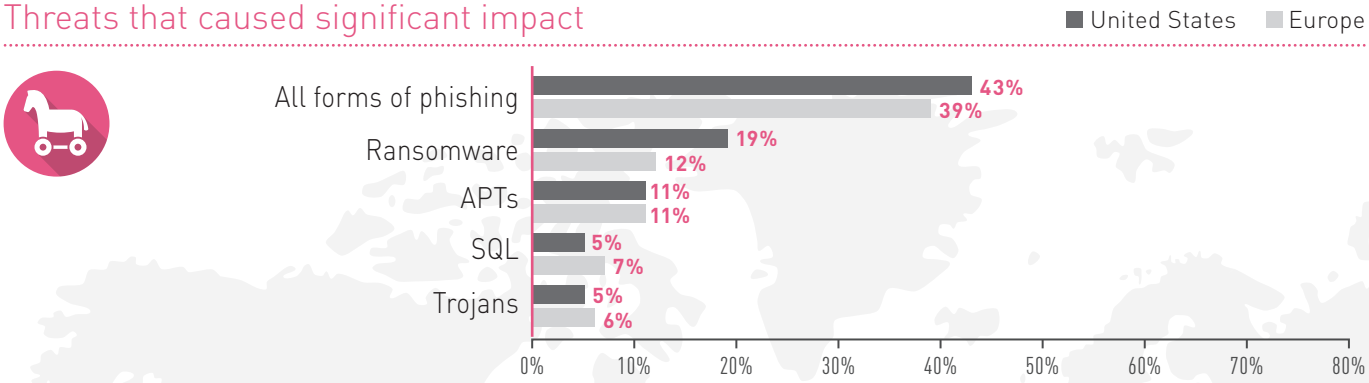
[2] 2016 BYOD and Mobile Security Report, Crowd Research Partners.
In the one out of five breaches, 39% were from downloaded mobile malware, and 24% were from malicious Wi-Fi networks.

KNOW YOUR ENEMY

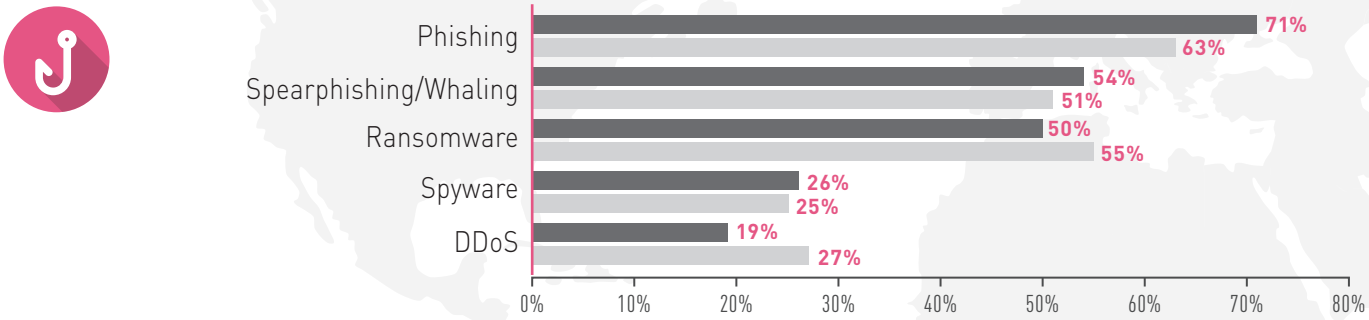
Strong defense—and offense—comes from knowing who or what the enemy is, and where it can come from. With that, below is a rundown of the different types of cyber evils organizations face—as well as how they're discovered.

Threats Manifested and Discovered – United States and Europe

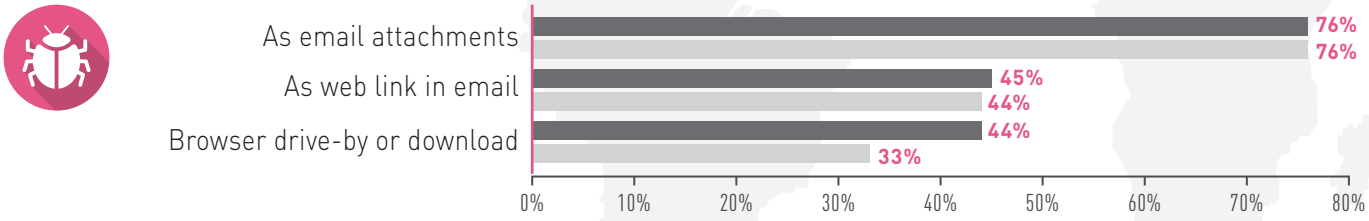
Threats that caused significant impact



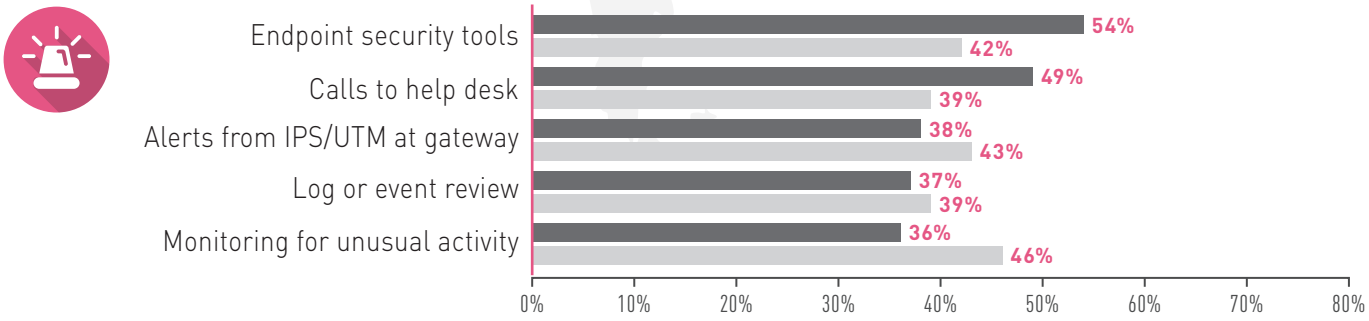
Threats on the rise



How impactful threats get in



How threats are discovered



Source: Exploits at the Endpoint: SANS 2016 Threat Landscape Survey

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.

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.

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.

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.

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.

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.

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

DLP (Data Loss Prevention or Protection): Protective software that operates based on policies and rules to prevent sensitive data or intellectual property from leaving an organization.

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.

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.

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.

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. Phishing that is conducted via short message service (SMS) texts is called SMS Phishing.

ACTIONS TO TAKE

Ask Questions

Begin by asking the right questions. Below are 10, which are adapted from questions provided by both Homeland Security[3] and CSO.com.[4]

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?

Have a Plan

Depending on what you learn from asking those questions, your next step is to either develop a new plan or retool the one you have. Central to this plan is communication. Leave nothing to chance or guesswork. Start with your data and assign access levels. Not everyone needs to have the same access. Map out who has access to what data and specify how it must be treated.

Keep it simple. Overcomplication is the biggest obstacle to security. When your policy is clear, more people align with it. And, when your security management is simple, it becomes easier and faster to keep things protected.

Make audits part of a routine. Make sure that you're not only compliant, but that your security measures are still performing as they should. Remember, any new technology or policy introduced into your security ecosystem can throw off something.

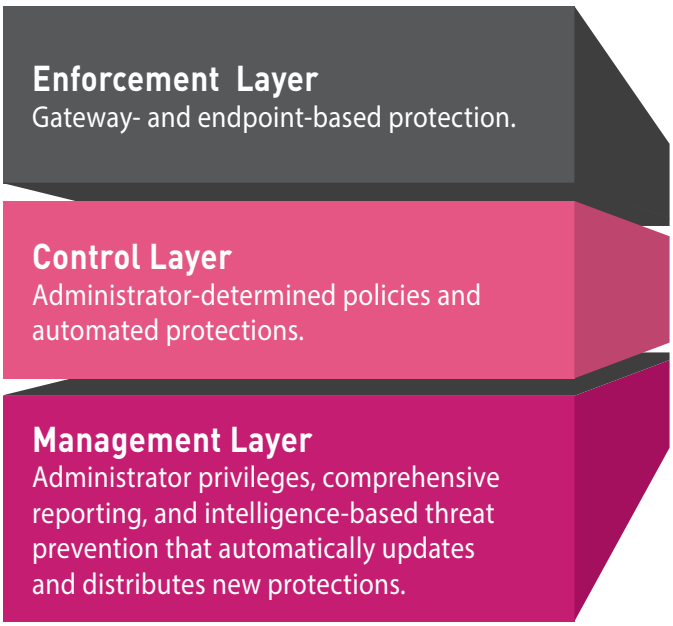
Identify a clear incident response plan. Include who needs to be notified, and the critical steps to follow should a breach occur. This helps to stem confusion and expedite the containment.

Think About the Big Picture: Your Architecture

When you think about the fact that all it takes is one threat to get in to wreak havoc—stealing information, knocking out productivity, tarnishing reputation—you want to be able to respond swiftly and effectively. Every second counts.

To build a secure architecture, the top rule is to simplify security management. That means managing all security functions, segments, and environments through one console. This ensures successful operations and smooth coordination of policies across network segments.

Make sure your architecture is environment agnostic, so you have threat protection that spans data centers, cloud platforms, software-defined data centers, SaaS, hybrid, and mobile environments. And with that, it's also critical to unify controls across all networks, systems, endpoints, and environments.



Think about your architecture as three interconnected levels: Enforcement Layer, Control Layer, and Management Layer.

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

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.

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.

Look for solutions that:

- Investigate any incoming file types
- Identify zero-day threats within and beyond the operating system
- Deliver documents safely, without malware and without delay
- 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 multilayered to automatically coordinate among different protections such as advanced threat prevention, security gateway, application control, antivirus, identity awareness, intrusion prevention, and URL filtering

The best way to manage your security is to implement a reliable monitoring and reporting process. If you can't see what's happening in your environment, you can't defend it. Make sure that your technology shows you what data is crossing your network and flags anomalies. In addition, take advantage of the reporting capabilities your technology offers. Studying patterns and being familiar with your network activity will give you important insights.

Defend and Train

To avoid outsiders gaining access to sensitive information, deploy data loss prevention strategies. These include:

Protection through Encryption
Whether at rest or in transit, ensure that only authorized individuals can see the data.

Protection through Checks and Balances
Keep access to data limited to a need-to-know basis based on pre-set permissions.

Protection through Education
Help everyone from top-down learn what behaviors are risky, what kind of information needs to be safeguarded, and how to recognize the traits of spearphishing or social engineering.

Protection through Separation
When it comes to mobile devices, create a barrier between sensitive work and personal data. This allows you to keep messages and files contained and encrypted. And, it ensures faster, easier management than with multiple devices and policies.

Protection through Training
Urge IT to set up cyber range exercises periodically. Using red team versus blue team scenarios, help staff learn to think like hackers so they're able to hone skills in how to react and respond to attacks.

Know How to Respond to Incidents—Timing is Everything

According to the 2016 IBM Ponemon Data Breach Study, it takes 201 days on average to identify a breach. But it doesn't stop there. The average time to contain that breach is 70 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, "While breaches that were identified in less than 100 days cost companies an average of $3.23 million, breaches that were found after the 100 day mark cost over $1 million more on average ($4.38 million)."[5]

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:

1. **Assess.** 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.
2. **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.
3. **Backup.** Make sure your team conducts a full backup, to capture the environment at the point of attack, to help with forensics.
4. **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.
5. **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.

MAKE IT WORK FOR YOU

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.

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 something that must be continually checked to ensure it is evolving to keep pace with the shifting threat landscape.

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

[5] IBM. "IBM & Ponemon Institute Study: Data Breach Costs Rising, Now $4 Million Per Incident." June 15, 2016.

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

Check Point®
SOFTWARE TECHNOLOGIES LTD

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

From its inception in 1993, Check Point's vision has been singularly focused on making internet services and resources secure and available for everyone. Our suite of market-leading solutions prevents attacks before they impact customers and provides unified management that hardens and streamlines security. Through continuous innovation, Check Point has become the world's largest dedicated cyber security vendor. This is how Check Point keeps customers one step ahead.