Business white paper

Cyber security best practices

Table of contents

The incidence and cost of cyber crime is escalating, and no business is immune. Attacks are more sophisticated and more successful, because hackers collaborate and share tools and techniques. So we must collaborate, too. In 2014, we sponsored a series of chief information security officer (CISO) roundtables, where participants shared experiences and enterprise security best practices. Through this paper, they are sharing them with you.

The problem

The number of successful cyber attacks in the U.S. has grown 144 percent in the past four years,[1] and the rest of the world is close behind. In that same time, the cost to the average company has almost doubled. On average, advanced attacks now persist in the network seven months before they are detected. And the time to resolve those attacks once detected has increased by 221 percent to 45 days.[2] Victims suffer financial losses, damage to brand, and damage to customer relationships.

Technology can detect and block attacks, but technology must also be applied by skilled people via thoughtful enterprise security processes. An effective cyber defense and response program must provide these, and chief information security officers (CISOs) must provide the leadership to plan, execute, and maintain an effective program. These best practices were shared by CISOs representing companies large and small in diverse industries and can help you mitigate the risks of a cyber attack against your organization.

[1, 2] "2014 Cost of Cyber Crime Study," Ponemon Institute, October, 2014.

The best practices

#1 Perform a risk assessment
The risk assessment is an inventory of data that could be stolen and services that could be disrupted along with an estimate of the cost your business would incur if those assets were compromised.

Why
Different kinds of data and resources have different values and represent different costs to the business if stolen or damaged. For example, marketing information is probably not as valuable to you as customer data. Because enterprise security resources will always be limited, you must plan your investment and manage your resources to offer the most protection to the data that if lost would yield the most damage.

How
Survey your systems to identify the data that could be stolen and the services that could be disrupted. Based on the amount and kind of data, estimate the cost to recover the data or mitigate the damage. Consider, for example, that you may have to offer customers credit and identity monitoring services if their data was compromised.

Success factors

- Engage business stakeholders in the process.
- Consider potential loss of revenue and brand damage.
- Establish priorities for protection and recovery.

#2 Develop an enterprise security plan

The enterprise security plan will contain your strategy and tactics for threat detection, response, and remediation. It should be keyed to the priorities and risks established by the risk assessment.

Why

Your plan guides your investment in security technologies and your hiring of security personnel. And it establishes processes for investigating suspicious activity, protecting resources, and responding to breaches. It's also your declaration to business leaders and other executives of how you will protect the company's assets and how you will respond if a breach occurs.

How

Different organizations have different planning processes, but any enterprise security plan must engage both stakeholders and functional experts to establish the right objectives and define how they will be met.

Success factors

- Define how you will protect assets, how you will detect threats, and how you will respond to breaches and suspicious activity.
- Focus resources according to the priorities established in the risk assessment.
- Be realistic; the plan must be aligned with the budget.
- Review and update it regularly.

#3 Put the right team in place

Skilled people are the most critical part of your cyber security program—and often the most difficult part to obtain. You must identify the skills and skill levels you need to execute the enterprise security plan, and you must establish the roles and responsibilities of each group and individual.

Why

Almost every system administrator or network engineer knows what to do if a system or network link goes down. But cyber security and intelligence are still part of an emerging career field, so you must know what you're looking for and hire carefully to create the core team you need to execute your plan and oversee the work of less qualified team members.

How

Recruitment and hiring practices vary from company to company. Start with a good understanding of the skills you need, and then assess candidates' abilities to execute your plan. Qualified, certified enterprise security professionals are in demand, so as you get the right people in place, be sure you offer them a work environment and development opportunities that will encourage retention.

Success factors

- Develop position descriptions, roles, and responsibilities based on your plan.
- Look for experience in the specialized, high-priority areas that loom large in your plan: mobile, cloud, application security, etc.
- Examine certifications of senior personnel. The most widely recognized is the ISC2 Certified Information Systems Security Professional (CISSP) for security professionals, but there are others, including vendor-specific certifications, which also indicate a good level of knowledge.

#4 Deploy defenses

Cyber defense technologies provide a number of enterprise security functions: They protect critical data by encrypting it; they detect and block attacks to stop them from penetrating the network; they detect successful breaches, so you can respond quickly to protect assets; and they enable security staff to investigate breaches and suspicious activity. When you develop software in house or through contractors, defenses also include the technology and processes to identify and fix vulnerabilities in the software, so hackers cannot exploit them.

Why

Expect to be breached; assume a breach has already occurred. No single cyber defense is 100 percent effective, so you must deploy defenses in layers that address all of the functions mentioned previously.

How

Hackers have become adept at evading defenses, but they leave tracks throughout the IT environment. Security technologies collect and analyze huge volumes of data and compare it to threat intelligence developed by security researchers like HP Security Research.

Devices like next-generation firewalls and intrusion prevention systems collect network data in real time and apply threat intelligence to detect attacks. Solutions like HP Advanced Threat Appliance watch for behaviors that indicate an attack was successful and an infection has occurred. Security information and event management (SIEM) systems amass data from log files and other sources throughout the environment, correlate it, and analyze it to detect attacks and to help the security operations team investigate and remediate attacks.

Success factors

- You need more than just firewalls and anti-virus. Deploy layered defenses that can block attacks at the network edge, detect and stop lateral malware communications within the network, and detect and remediate successful breaches.
- Select enterprise security solutions that leverage the best threat intelligence available.
- Collect as much data from the environment as you can.

#5 Respond to incidents

When a breach occurs—and a breach will occur—you must respond to protect critical assets (as prioritized in your plan); to stop the attack or at least quarantine infected systems; to plug the vulnerability hackers exploited (remediate); to collect and preserve data that could be used as evidence in criminal proceedings; to communicate with impacted customers, employees, and others; and to fulfill any legal responsibilities.

Why

The speed and effectiveness of your response determines how much damage you will suffer. Research shows the average time to resolve a cyber attack in U.S. companies is 45 days at a cost of almost $1.6 million USD per incident.[3] More significantly, hackers may continue to exfiltrate data until the attack is completely stopped. Further, you will be subject to legal requirements for notifications to impacted customers, partners, and law enforcement authorities.

How

You must execute your enterprise security plan for incident response. Team members and others in the organization must know their responsibilities and how to discharge them. Processes should cover everything you must do, but must be kept simple enough to execute flawlessly. Legal and communication obligations should have been identified and planned for in advance.

[3] "2014 Global Report on the Cost of Cyber Crime," Ponemon Institute October 2014.

The most pressing action is to remediate—stop the attack by closing vulnerabilities in code, blocking the attack, or quarantining infected systems. Post recovery, you must assess the damage, perform any needed communications, identify lessons learned, and feed learnings back into your security plan.

Success factors

- Practice your incident response plan before you have to execute it for real.
- Identify and correct inadequacies in the plan.
- Apply accepted forensics techniques to preserve evidence.

Conclusions

CISOs who participated in these roundtables agreed the key to better cyber security and intelligence is thoughtful planning and consistent execution. These enterprise security best practices are high level, and the devil is surely in the details. But there are key takeaways that should drive the thinking behind every security program:

- Identify your most valuable assets and protect them by encryption and other data security means.
- Deploy layered defenses that detect and block attacks at the network edge, detect lateral communications within the network, detect successful breaches and quarantine infected systems, and provide the data needed for investigation and remediation. If you develop your own software, scan it for vulnerabilities prior to release.
- Tap into the best threat intelligence available. A security solution is only as good as the threat intelligence behind it.
- Collect and analyze as much data as you can to find the needle in the haystack that indicates hackers are at work.

Resources

- HP security solutions include HP TippingPoint network security solutions
- HP Fortify application security solutions and cloud-based services
- HP ArcSight Security Information and Event Management
- HP Atalla data security and encryption solutions

They are backed by threat intelligence from an industry-leading research program, HP Security Research, with more than 3,000 HP and independent researchers looking for vulnerabilities in the software you use. HP Security Consulting Services help organizations like yours around the world plan and execute the enterprise security programs to make their businesses safer.

Learn more at
hpenterprisesecurity.com

Sign up for updates
hp.com/go/getupdated

✉ Share with colleagues

★ Rate this document