Foresight
Innovative Solutions

10 ways to develop cybersecurity policies and best practices

10 ways to develop cybersecurity policies and best practices

Today's security challenges require an effective set of policies and practices, from audits to backups to system updates to user training. Here are 10 ways to make sure you're covering all the bases.

In January 2018, UK businesses were victimized 7,073,069 times. On January 3, 2018, the US Department of Homeland Security informed 247,167 of its employees that their data had been breached.

It's been an auspicious beginning for cyber hackers in 2018, so it comes as no surprise that security and risk management were rated as the number one priority for CIOs in a November 2018 NASCIO survey.

But are companies ready?

"We are in the fifth generation of cyber security," said Gabi Reish, vice president of marketing at Check Point, a security provider.

Reish lists the cybersecurity generations as follows:

Gen 1: Developed when PCs with floppy disks were first introduced in the 1980s, with viruses as the first cyberattacks.

Gen 2: Emerged during the mid-1990s, with cyberattacks focused on data and network security; the solution was firewalls.

Gen 3: Began in the early 2000s with the exploitation of applications, browsers, and networks. This was the beginning of network intrusion detection.

Gen 4: Began around 2010, with more sophisticated cybersecurity attacks that embedded malware in email, documents, and images. This generated security technology that 'sandboxed' these occurrences to contain them and prevent them from spreading to other areas of the network.

Gen 5: Broad-scale attacks that involve ransomware, phishing, content exploitation, and/or any number of combinations.

Unfortunately, Reish also says that most companies "are only at generation two or three" cyber protection levels, and a recent survey by Radware, which provides DDoS attack prevention, firewalls, and network load balancing solutions, supports this. According to the Radware survey, "Despite one in four (24%) businesses reporting cyber-attacks daily or weekly, nearly 80% of surveyed organizations have not come up with a calculation for the costs of attacks, and one in three lack a cyber emergency response plan."

One approach to tightening up cybersecurity is to implement the most effective technologies -- but those technologies are only as effective as the companies and people who operate them. This makes policy setting and enforcement a paramount objective for CIOs and CSOs.

So what are the best ways to go about developing sound cybersecurity policies and practices in 2018? Here are 10 recommendations.

1. Update software and systems

After Spectre struck in January 2018, Apple issued security fixes for its iOS 11 operating system. This is no different from what other IT vendors do when they discover a security vulnerability. However, the rub for IT is making sure that the diversity of devices that are in the hands of users are all updated with the latest versions of a bevy of OSs. This requires centralized policy making in IT that likely adopts a 'push' methodology, forcing new security updates onto a user's device when they connect to the network, instead of a 'pull' methodology, which notifies the user that a new security patch is available and gives them the option to load this new software when it's convenient.

We have been a proponent of pull updates to software in the field because you never know when a user needs their device, and these updates can get in the way. But the volume and velocity of today's cyberattacks require tougher guidelines, since it is also true that many users never bother to pull an update to their devices. Consequently, in 2018's security environment, push is the surest security protection policy.

2. Conduct top-to-bottom security audits

If your company hasn't already done so, it should conduct a thorough security audit of its IT assets and practices. This audit will review the security practices and policies of your central IT systems, as well as your end-user departments and at the 'edges' of your enterprise, like the automated machines and IoT you might be employing at remote manufacturing plants. The audit should look not only at the software and hardware techniques you have in place to protect security but also at remote site personnel habits and compliance with security policies.

3. Don't forget social engineering

As part of your end-to-end IT audit, you should include social engineering, which reviews whether your employees are demonstrating vulnerability when it comes to offering up confidential information.

This social engineering can be as simple as someone shouting a password to a co-worker over an office partition -- or it could be a user who pulls up a website at work and surrenders passwords or other vital information that ultimately gets into the wrong hands.

"Requests for social engineering audits have increased," said Stuart Chontos-Gilchrist, CEO of E3 Technology, an IT security audit firm. "Companies are recognizing that it is people, more often than machines, who generate security breaches."

4. Demand audits from vendors and business partners

According to a 2017 report by Commvault and CITO Research, more than 80 percent of companies see the cloud as integral to their technology. But with the move away from internal data centers, it's also become more important to demand regular IT audit reports from your vendors and business partners. Companies should have policies in place that require regular security audit reports from vendors they are considering before contracts are signed. Thereafter, vendors, as part of their SLAs, should be expected to deliver security audit reports on an annual basis.

5. Provide new and continuing security education

Cybersecurity education should be a staple of every new employee orientation, with new employees signing off that they have read and understood the training. On an annual basis, a refresher course in cybersecurity practices should also be given to employees company-wide. This ensures that security policies and practices stay fresh in employees' minds, and that they understand any policy additions or changes.

6. Watch the edge

Manufacturing 4.0 and other remote computing strategies are moving computing away from data centers and out to the edges of companies. This means that a manufacturer with a remote plant in Ireland is likely to have manufacturing personnel operate automated robots and production analytics with local servers in the plant. Software and hardware security must be maintained on these devices, but the devices must also be locally administered under accepted cybersecurity policies and procedures by personnel who are asked to do these jobs without an IT background. This is a security exposure point for the company and for IT that requires training of non-IT personnel in IT security policies and practices, as well as oversight by IT and auditors.

7. Perform regular data backups that work

If your data is compromised or held hostage in a ransomware attack, a nightly data backup will at least enable you to roll back to the previous day's data with minimal loss. It's a simple enough policy and practice to enact. Unfortunately, a bigger problem for companies is not so much that they don't perform data backups -- it's that the backups don't always work. One of the most important cybersecurity policies that corporate IT can put in place is a requirement that data backups and disaster recovery minimally be full-tested on an annual basis to ensure that everything is working properly.

8. Physically secure your information assets

Even if software, hardware, and network security are in place, it doesn't help much if servers are left unsecured on manufacturing floors and in business units. Physical security, like a locked 'cage' for a server in a plant that is accessible only to personnel with security clearance, is vital. Security policies and practices should address the physical as well as the visual aspects of information.

9. Maintain industry compliance

Especially for companies in highly regulated industries like healthcare, insurance, and finance, regulatory compliance that concerns IT security should be closely adhered to. Companies in these industries should annually review security compliance requirements and update their security policies and practices as needed.

10. Inform your board and CEO

A successful cybersecurity strategy is one where you never find yourself in front of the CEO or the board having to explain how a cyber breach happened and what you are doing to mitigate it. Unfortunately, great security systems are 'invisible', because they never give you problems.

This makes it important for CIOs, CSOs, and others with security responsibilities to clearly explain cybersecurity technologies, policies, and practices in plain language that the CEO, the board, and other nontechnical stakeholders can understand. If the non-technical people in your organization can't understand why you are enacting a certain policy or asking for a sizeable investment for a cybersecurity technology, you're going to have trouble making your case -- unless you're all suffering through an embarrassing security breach that could end careers and put the entire company's survival on the line.