Have you checked your security posture?

Staying safe in a shifting, dangerous threat landscape

Table of Contents

02
A day in the life of security

03
Keeping your security posture healthy

04
10 technical and logical controls to increase your position of defense

08
Solidifying your path to better security

FLEXENTIAL

A day in the life of security

This is the world we live in: attack attempts, newly discovered vulnerabilities and methods for gaining unauthorized access crop up on a daily basis. Massive breaches and compromised data among the enterprises we interact with regularly have become a commonplace part of the morning news.

According to Cisco, malicious actors have more means to execute attacks than ever before, and their intuition for timing is growing. While online traffic and mobile endpoints multiply exponentially, hackers gain a broader range of targets and innovative methods.[1]

- 49% of security professionals surveyed in the Cisco 2017 Security Capabilities Benchmark Study reported having to manage public scrutiny following a security breach.
- Nearly 25% of organizations who suffered an attack lost business opportunities as a result. 40% said those losses are substantial. One in five organizations lost customers because of an attack, and nearly 30% lost revenue.
- When breaches occur, the following functions are most likely to be impacted:

26%	26%	36%	30%
Customer retention	Brand reputation	Operations	Finance

There's no denying that we're operating in a heavily risk-laden environment. It can be nerve-wracking for any business to evaluate its security posture given the landscape of today, but the good news is that there are definite ways to be as prepared as possible, starting with knowing how and why you could potentially be compromised.

"Why us?" - reasons you could be compromised

Let's start with the burning question of any business who has suffered a breach: "Why us?" There can be a number of reasons behind an attack. Here are the ones we see most commonly:

Opportunistic attacks

There are a multitude of unethical agencies out there that get paid to look for holes in systems, gather data, or serve as the middleman in a larger scheme. Hacking can be akin to a kind of sport or achievement in the "because we can" bucket for some malicious actors. It earns them internet street cred.

Targeted attacks

Motivations vary, but sometimes an attack is the result of a very deliberate effort targeted at a specific organization. Large, well-known organizations are certainly at risk. Again, the lure might be simply for notoriety, or it could be to obtain very valuable personal data. It could be related to an organization's activism, or conversely, the cyber attackers' leanings.

If you're not a large, well-known organization, don't think you're immune to targeted attacks. Have you ever had a disgruntled employee? Or do you think your competitors are above playing dirty? Targeted attacks can occur more often than you think.

Absent controls

Controls, or safeguards, are necessary to prevent and detect and attack, as well as to minimize the damages. Security is really built in layers; you can't just have one control in place. Organizations leave themselves open to a breach if there are failings in one or more controls, or if they're insufficient.

Controls are why it's important to have a strong team, either on the payroll or on retainer, closely working to maintain security practices across your organization in order to protect the confidentiality, integrity, and availability of your information.

Bad luck

Sometimes an attack is the result of zero-day vulnerabilities: "bad luck," for lack of a better term. Of course, no one can predict when these types of incidents will occur. However, steps can be taken to minimize the damage that these attacks can cause and restore operations as quickly as possible.

It's important to understand the reasons why your organization might be at risk. Security isn't about a tool, a person, or a product. None of that will solve the problem or reduce worry without having an in-depth, internal conversation. Security is about educating and performing due diligence. Only then can you defend, protect, respond, and investigate.

[1] [Industry Report]: Cisco 2017 Annual Cybersecurity Report. Cisco. Retrieved October 27, 2017 from http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017.

Keeping your security posture healthy

Maintaining a healthy security posture means being proactive from both a human and technology standpoint - it's not one or the other.

The technologies to protect critical IT assets are constantly evolving, but so are the threats, and achieving a healthy security posture requires a dual effort shared by both people and technology. According to the Ponemon Institute, human error is responsible for 22% of outages.[2]

To provide a higher level of assurance and protection against data loss, both from inside and outside sources, companies must invest in people as well as technologies and processes.

People controls - what you and your organization can do

Know your assets

You can't protect what you don't know. The cornerstone of a healthy security posture is knowing your assets so that you know exactly what you're trying to protect. It's what allows you to ensure all the right controls are in place, so you should have a complete inventory. Then comes protecting against the threats that accompany your specific assets. If you have old firewalls or a vulnerable application, select the right tools for proper protection.

Understand your risk profile

Knowing your risk profile is key. You need to know the risks specific to your industry, business, and assets. To get started, you can begin a simple information-gathering process on the internet. Look up your company name and see what kind of information can be gathered. If possible, engage with a professional penetration tester. Also be aware of your unique exposure and visibility. If it's obvious on your website that you service credit card companies, then you have higher risk, for example.

Documentation is a critical component of fully understanding your risk profile. Over time, especially in legacy environments and through job changes, original information can be lost. Without proper documentation, risk gets higher, not only from a security perspective, but from an availability perspective in the event that a system goes down.

Lastly, execute a security assessment. If you haven't done one or brought in a third party to evaluate your perimeter, controls, and monitoring, you may not be making the best use of your tools for your environment, which again, increases risk.

Have a solid risk management program

Do you have a risk management program? By default, you should be carrying out annual risk management reviews, complete with a repeatable process and scoring. This assists leadership in determining overall risk and potential costs to the business in the event of compromise or breach, which enables the ability to appropriately allocate funds to reduce or mitigate business-specific risks.

Tip: At the end of the day, you need to determine if you're going to accept or reduce risk. You can reduce risk by adding security controls, or accept it by determining that risk is low enough not to invest additional funds at that given time.

[2] (2017, June 21). IBM | Ponemon Cost of Data Breach 2017. Retrieved October 27, 2017, from https://www.ibm.com/security/infographics/data-breach/

FLEXENTIAL

Keep your information security program up-to-date

As you make your way through the above steps, it's likely that you'll find it's time to update your information security program once again, which includes your information security policies. It's recommended to maintain one primary information security program and update it every six months to one year as a formal, recurring process. This way, all of your procedures and standards can be matched with the program, allowing you to train your company through awareness.

Make sure leadership is involved

Leadership has to be involved in decision making. Without deliberate planning, security often happens in silos, which hurts the culture of your company. If you don't promote awareness and bring leadership into the conversation, trying to get more budget or communicating risk to users can be difficult.

Put together a security board

Put together a security board of ambassadors. There should be a security ambassador for each department working as the liaison between the security team and other departments and business units, which allows for healthy two-way communication.

10 technical and logical controls to increase your position of defense

We've covered human controls, but what about controls that are technical and logical in nature? These are types of measures which need to be configured within your systems, applied, and relied on to collectively reduce risk to the environment. Ultimately, you want to ensure that existing vulnerabilities are mitigated in a timely manner and the threat profile of your organization is lessened.

It's worth noting, while the risk landscape is much greater today than five years ago, we're in a much better position with regard to tooling and capabilities around automation, whether for deployment, maintenance, or ongoing monitoring of controls. In the past, assessment of technical controls was a more stressful, time-based exercise. Today, we have the ability to monitor on an ongoing basis and more easily observe how controls are performing, as well as where there may be room to improve.

Reported by Cisco, much of the focus of your defense strategy should be reducing your adversaries' operational space. This makes it much harder for malicious actors to gain access to resources and carry on undetected, which is where automation comes in. It helps delineate normal versus suspicious activity within your network environment, and that enables your internal security resources to resolve legitimate threats, rather than diverting them with false alarms.

> **"Only with automation can security teams cut through the "noise" of security alerts and focus their resources on investigating true threats. The multistage process of identifying normal and potentially suspicious user activities […] hinges on the use of automation, with algorithms applied at every stage."**
>
> **- Cisco, 2017 Annual Cybersecurity Report[1]**

01 Patching

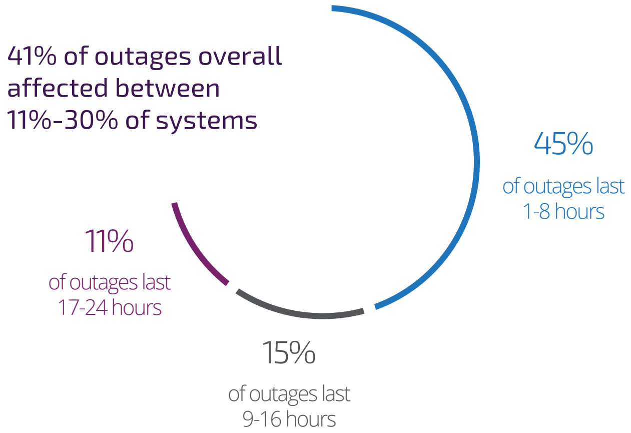
According to Cisco:

Regular and predictable update schedules lead to users upgrading software sooner, which lessens the time window during which malicious actors can take advantage of vulnerabilities.[1]

Patching is an essential security control, without a doubt. Patching your operating system is important, but don't neglect other areas of your environment that run code, either. This includes infrastructure devices and applications that run on top of your operating systems. Don't forget, common vectors of risk today are often user-dependent, which means you need to address all infrastructural layers where users interact with systems.

Monthly security patching is recommended. Quarterly is no longer adequate, especially from a service interruption standpoint. Inadequate patching can result in unplanned outages, so fast, responsive patching is key.

Network outages caused by security breaches can have an ongoing impact. As determined by the Cisco Security Capabilities Benchmark Study:



Tip: Don't overlook vendor security notices. Managing systems alerts is important, but don't forget to subscribe to vendor notifications and vulnerability announcements, too.

02 Lifecycle management

At some point, vendor support for security is lost, and as systems age, functionality and standards related to communication within environments can wane. Legacy systems prevent a very real risk, and in only takes one event and a highly vulnerable piece of equipment. Keep pace with lifecycle management related to all layers of your stacks: physical devices, infrastructure devices, operating systems, applications, database services and systems; they all require a strategy to manage the lifecycle.

03 Robust firewalling

- Avoid using overly permissive firewall rules
- Use web application firewalls
- Perform regular firewall rule reviews

Avoid using overly permissive firewall rules. Often times, rather than trying to engineer or determine specific communication requirements, rules are hastily written and overly permissive; in some cases, between private connections, or even public connections, usually just because there's an urgent business need to get a service deployed. Maybe a particular technician had the intention of coming back to resolve or tighten the rule set, but forgot. Scenarios like this can happen and result in an unresolved rule that is in place for months or even years.

Using web application firewalls is a less common defense tool, and it may not be applicable to every organization. However, if you have a web presence, are hosting websites for your organization, or are dealing with customer transactions, a web application firewall can serve in a very similar capacity to a web proxy, whereby it inspects connections coming in, and can evaluate for characteristics that seem high risk.

Lastly, don't forget to perform regular firewall rule reviews. Ensure that tight rules are in effect and only permit what is actually required for a given service.

04 Employ best practices for passwords

- Use strong, complex passwords
- Use multi-factor authentication

Attackers often use default or stolen credentials to make their way around a network, Symantec explained. Passwords being used for high privileges need to be 8-10 characters long at minimum, including both letters and numbers.[3]

This recommendation may seem obvious, but it's still worth mentioning. Believe it or not, much of the world has continues to neglect strong password practices security. Encourage employees to use, strong, complex passwords.

Also, while it's becoming less common, there are still some vendors and providers of applications and equipment that deliver systems with default configurations that don't come close to meeting best practice standards today. Therefore, evaluate new services and systems before deployment and ensure their defaults align with what you're willing to accept from a configuration or risk standpoint.

Tip: Use multi-factor authentication. Today, the standard password on its own, even if it's strong, is not enough. When it comes to remote access of any kind into your environment, multi-factor authentication is a best practice and a must-have. It's also worth deploying for higher-risk systems and infrastructure management systems—things like management switches, routers, and firewalls.

05 Be as proactive as possible

- Use web proxies
- Utilize anti-malware and anti-virus tools
- Encrypt

Web proxies are a very important part of environments. If you have more than a handful of users, you're not so much monitoring for users' web browsing behavior as you are providing a chokepoint for traffic analysis. You should be monitoring the behaviors and sites that users are visiting to enable the proxy to provide security response features. This way, it can quickly update from signature databases of known, high-risk sites. For instance, if a user clicks a link in their email related to a phishing attack, this proxy serves as another point of control that can help mitigate risk.

Anti-malware and anti-virus tools are as essential today as they were a decade ago, although the approach to how those are being used is starting to evolve slightly. More products take less of a signature-based approach to protection, emphasizing heuristics, behavior, and how code is interacting with the operating system.

06 Network access controls

Monitor unusual access activity

A firewall no longer equates to security. The network access control mentality has to extend into your network, and you shouldn't fall victim to the idea that internal networks are trusted—any traffic from any source is potentially suspect.

Some organizations even take the approach of assuming all traffic on the network could be from compromised hosts because of the challenges of securing the network access layer in large organizations. Managing wireless access and using firewall rules are ways to limit wireless access based on need; so is using authentication to prevent or to permit users onto specific networks.

Tip: Monitor traffic. There are tools that enable us to do this very effectively today and even proactively respond. IDS and IPS (sometimes termed IDPS) help monitor network traffic based on patterns, signatures and known risks that are being updated as part of a subscription feed that can then help mitigate some of that higher-risk traffic in both directions.

[3] [Industry Report]: Internet Security Threat Report. Symantec. Retriever October 27, 2017 from https://www.symantec.com/security-center/threat-report.

FLEXENTIAL

07 Enforce policies and proceduresv

- User awareness training
- Have a plan for when things go wrong

Enforcing policies and procedures is essential. You should be monitoring things that employees are doing from an account usage perspective. Also ensure that they're following practices that have been defined to help reduce risks to the organization.

This includes things like training and following up with unruly users with disciplinary action and additional training. It may sound extreme, but if you're not correcting risky behavior and making it clear organization-wide that stakes are high, there is less incentive for employees to pay attention, and they may be more inclined to take shortcuts and potentially increase risk to the organization.

Also, move away from the monotonous annual slew of compliance slides and look toward more interactive, tailored training models that will add value to the effectiveness of training programs.

Have a known plan for when things go wrong, as well. You can't plan for everything, but you can have a starting point of response for when something happens. Everyone should know the series of steps to follow to get a handle on a potential incident and reach a safe conclusion.

08 Backups and disaster recovery

Backups are essential. The way you go about backing up and storing data heavily impacts your security. Today, there are multiple options that include snapshotting, replication, cloud-based backups, off-cloud backups, and traditional tape backups. Choose what works best for you.

Don't forget to have a formal plan, too—especially given the dominance of ransomware. If you're exploited, your best chances of getting your data back is backup recovery.

Similar to backups, have a DR plan. How are you going to use backups in order to recover systems? What's the relative criticality of systems, and which ones will you need to restore first? If your data center flooded tomorrow, what would happen to your business? What would you need to do in order to recover, and do you have reasonable plans in place to do so?

09 Provision appropriate administrative access levels

Create secondary accounts for admins

You do not need 20 systems administrators in your organization. Define the roles people need to perform, and grant access that's appropriate to their position—not above and beyond what they need. Don't take the easy way out for provisioning access.

Tip: Secondary accounts are an absolute must. Your admins should not be using the accounts meant for web browsing and viewing email as administrative accounts. If an administrator has a need to administer systems, they should have a secondary account.

FLEXENTIAL

10 Maintain control of your environment and its activities

- Periodic environment scanning
- Application log review

You should be periodically scanning your environment on a monthly basis. You need to know your risk profile, and the more you scan, the sooner you can identify vulnerabilities and mitigate the risk associated with those. Perform scanning for both your external IP address as well as your entire internal network, which provides insight into how you're doing from a compliance standpoint with controls.

Also, execute application log reviews. Recently, there's been great progress in terms of collecting logs, but actually using them is still fairly uncommon. They are often used for retroactive incident review, but there's less of a mentality around having a process or tooling in place to support automated review of logs. Consider SIEM solutions that can analyze logs and react based on pre-defined patterns or behaviors.

Solidifying your path to better security

Businesses are experiencing a high level of concern – and even panic – given the threats we're all facing as businesses. Thankfully, there are proven approaches for minimizing the fear and risk. In many cases, the universal struggle is cost versus security. Many businesses can't foot the full cost of maintaining security in-house. In other cases, knowing where to start is a challenge. Only you know the amount of security risks and types of data you have. If you don't have a robust, proven security team available internally covering every aspect of your security posture, it makes sense to consider a professional services team, or even partnering with a secure, managed hosting provider. Remember to ask comprehensive questions regarding the security controls they can provide, and confirm that they provide support for auditing and compliance, whether your intention is to self-manage or outsource. Regardless, all of the human and technical controls as listed above should be covered.

"We can't control everything, but in many cases, security breaches are preventable. The key is to protect in layers because security is built in layers. You can't just have one security control and think you're safe. You need to have several layers, and you need to be prepared."

Annalea Ilg
Vice President & CISO
Flexential

Flexential helps organizations optimize IT transformation while simultaneously balancing cost, scalability, compliance and security. With a focus on building trusted relationships, providing valuable support and delivering tailored solutions and reliable performance, Flexential delivers colocation, connectivity, cloud, managed solutions and professional services to 4,200 customers across the U.S. and Canada.