Dealing With Cybersecurity Threats When Resources Are Limited

ConRes
IT SOLUTIONS

The Cybersecurity Challenge for Businesses Today

According to the Online Trust Alliance (OTA), the number of cyberattacks targeting businesses doubled between 2016 and 2018.[1] OTA estimates that there were 159,700 successful cyber incidents in 2017, or one every three minutes. The number of attacks might be much higher, as many incidents and breaches go unreported or undetected.

Spending on security is growing right along with the number of attacks. Gartner expects global spending on cybersecurity to reach $93 billion in 2018.[2] Cyberthreats used to be a problem that only governments and larger enterprises had to worry about. That is no longer the case. Every organization is a target.

Complicating the issue even further is the lack of qualified cybersecurity expertise. According to Cybersecurity Ventures, there were nearly 780,000 people employed in cybersecurity positions in 2017 in the U.S. But there were another 350,000 cybersecurity job openings.[3] That skills shortage is expected to grow to 3.5 million unfilled cybersecurity positions worldwide by 2021.

These numbers paint a pretty bleak picture. So, what are organizations with limited resources supposed to do to protect themselves, their data, and their employees? Let's take a closer look.

One every 3 minutes

OTA estimates that there were 159,700 successful cyber incidents in 2017, or one every three minutes.

1 Online Trust Alliance | Cyber Incident & Breach Trends Report | https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
2 Gartner | https://www.gartner.com/newsroom/id/3784965
3 Cybersecurity Ventures | https://cybersecurityventures.com/jobs/

Start With the Essentials

The alarming news, according to Online Trust Alliance, is that up to 93% of all breaches in 2017 could have been prevented with simple cybersecurity best practices.[1] That includes updating software, applying patches, hardening systems, blocking fake emails, and training employees to recognize phishing attacks.

The highest-profile cyber incident of 2017 was the data breach at Equifax, where the personal data of 143 million people was compromised. Hackers exploited a known vulnerability in an Equifax Apache web application. Disturbingly, a patch for the vulnerability was available for two months prior to the attack but was not applied.

Mitigate Vulnerabilities

There have been a couple of major vulnerabilities reported this year. Meltdown and Spectre vulnerabilities can be harnessed by hackers to read sensitive data directly from the CPU. These vulnerabilities exist in nearly every processor sold in the last 20 years.[4] Patches have been issued, but those patches are only useful if they are applied.

Staying up to date with security patches, along with using basic tools such as firewalls, access control, identity management, and malware protection, is a good start — but it is not enough. Hackers continue to become more sophisticated. And at the same time, a ton of data now lives outside the network and in the cloud.

What else can you do to improve your security posture?

Almost all breaches are preventable.

Up to 93% of all breaches in 2017 could have been prevented with simple cybersecurity best practices.

4 CNET | https://www.cnet.com/news/spectre-meltdown-intel-arm-amd-processor-cpu-chip-flaw-vulnerability-faq/

A Unified and Layered Approach to Security

It is important to note that there is no silver bullet for security. There is not one single tool, or even a suite of tools, that will protect you from every threat. With so many potential points of vulnerability, it is imperative that you adopt a layered security approach. Layered security uses multiple controls to secure your data to mitigate single points of failure.

First you need to understand the data that your organization has, where it is stored, and who has access to it. You cannot protect what you don't know you have. Many businesses are surprised to learn that they have many copies of their sensitive data in many locations — even in places they didn't expect, like within the development team.

Define the types of data that you have. Know which data is sensitive and identify the controls required to protect it. This is something that every organization must determine for itself. You need to evaluate the risks associated with that data versus what it will cost to protect it. For instance, which data needs to be encrypted and when? Which data should be encrypted at rest, in transit, or in use?

Security Principles

There are several principles that you can refer to when deciding how to secure your data:

- **Need to Know:** This is the key component of any security system. Grant data access only to the people and users who need it for processing or decision-making.
- **Least Privilege:** User accounts run with the fewest number of privileges, or access to data, required to complete the job they are doing.
- **Separation of Duties:** This principle means that you are restricting the amount of power that any individual has over your data. Security is spread across multiple people to limit the damage they can do.

The key to remember is that the greatest threat your data faces is from people's action, or failure, inside your organization.

Now you need a way to monitor and understand what is happening on your network.

There is no silver bullet for security.

Make Full Use of SIEM

Does every organization have to implement a Security Information and Event Management (SIEM) system? Probably not. But if you are looking to improve your security posture — which we assume describes you since you are reading this eBook — then you will most likely benefit from a SIEM system.

What is SIEM? There are many definitions. At a very basic level, it is a set of technologies that give you a holistic view into your infrastructure. This is critical as you implement a layered approach to security so that you can understand what is happening at every level and act on that data.

It is important to note that SIEM is not a plug-and-play solution. For SIEM to be effective, it has to work on a business-process level as well as a technical one. Your SIEM system will get better over time as more data is collected.

SIEM and Analytics

SIEM systems are getting smarter. Instead of just recording and reporting what is happening in your environment, modern systems use data analytics to act on anomalies and perceived threats. For example, it can instruct the network layer to isolate a user that is behaving abnormally.

Your SIEM can be further enhanced by leveraging threat intelligence. Threat intelligence takes known threat information and transforms it into intelligence. Your system then recognizes the behavior of threats and shuts them down. By using threat intelligence, you can reduce the amount of time spent analyzing logs trying to identify an attack.

The topic of SIEM and how to implement a system successfully is a complex topic, and beyond the scope of this article. Upon successful implementation, a SIEM system can enhance your security posture and help it to mature over time.

What do you do when you have a security incident or breach?

A SIEM system can enhance your security posture.

Have an Incident Response Plan

Many experts say that it is not *if* your organization will be a target of a cyberattack, but *when*. You should have an incident response plan in effect so that you and your team know what to do when you discover you have become the victim of a cyberattack or breach. That is not the time to try and devise a response plan – preparation is the key.

Determine up front what specific laws and policies will apply in case of a data breach. There are guidelines that are either set by law or featured in your company's privacy policy.

For example, in spring 2018, most people received a lot of privacy policy updates due to Europe's new data law, the GDPR. The law applied to not only European companies but also any organization that does business with specific European data. The law requires that users be notified in the event of a breach and specifies the deadline in which to do so.

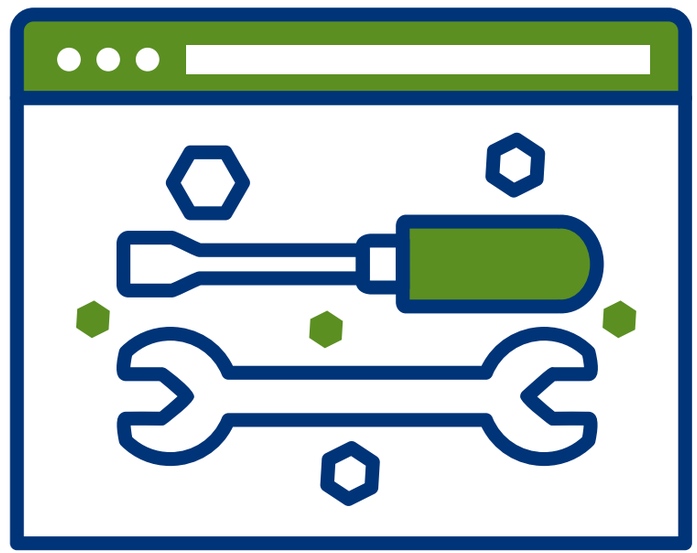
Know What You Will Do and Who Will Do It

Prioritize and plan for attack scenarios. Ransomware attacks, for example, are on the rise, and every organization is a potential target. The only way to protect your organization from a ransomware attack is to thoroughly plan how you will respond if a hacker locks up your data and demands a ransom.

You need to define who your incident response team members are and train them on how they will respond. This includes the lines of communication. You should have clear document guidelines for all responding parties, administrators, and staff. Then, practice those plans so you know you will be ready when under the stress of an attack.

This may sound like a lot for an IT team or a security response team that is already stretched thin. How will you prepare for and protect yourself from cyberattacks?

Preparation is the key.



Conclusion

This guide is intended to stimulate your thoughts about multiple areas of cybersecurity and the steps that you can begin taking today. Unfortunately, there is no magic formula to be instantly protected from cyberattacks. Not yet, at least.

Cybersecurity is a perpetual process that never ends, because threats are always evolving. What is important is to begin your journey. Over time, your security posture will mature, and you will be more prepared to protect your organization from threats.

Cybersecurity is not just a technical challenge, but it is also a business challenge, … and the entire organization needs to be on board. As your security matures, protecting data should become a part of your organization's culture, from C-Suite on down.

Don't Worry, You Don't Have to Go After It Alone

The cybersecurity experts at Continental Resources (ConRes) are here to help. We use our combination of over 50 years of technology and business expertise to guide you on your security journey.

Don't worry, you don't have to go after it alone.

Contact us to schedule a free Security Discovery today.

ConRes
IT SOLUTIONS