WHITE PAPER

10 Steps to Proactive Security

solarwinds

It has become commonplace to say the state of cybersecurity has changed. It's true—cybercriminals continue evolving their methods of attack. It's not just malicious actors you have to worry about either—with the world growing more interconnected, it's more likely than ever that insiders will accidentally cause a data breach.

To see how serious the state of cybersecurity has become, just look at some of the breaches from 2017. The Equifax® breach led to a loss of over 143 million personal records[1]. This happened to a company that protects private, personal data—just imagine how challenging it is for those with fewer security resources than Equifax. And with ransomware attacks like Petya, WannaCry, and Bad Rabbit, cybercriminals no longer have to steal data records to succeed with cyberattacks. They can simply lock up data and hold it hostage for a time to wreak havoc (and gain financial benefit).

What the industry needs is a sea change in how we think about security to enable us to more proactively fight cybercriminals. This whitepaper outlines ten steps to help get there.

What the industry needs is a sea change in how we think about security to enable us to more proactively fight the cybercriminals.

1. SHIFT THE CONVERSATION TO RISK

No business is ever 100% secure. You can have the best security technology and processes in place, but there's always the risk that a new type of attack could hit your company first. Yet, the conversation often focuses on an almost binary view of either being secure or not. This all-or-nothing proposition denies the reality of the situation.

Instead, you should focus on risk. Most businesses already think about general business risks like bad press or changing market demand—cybersecurity should be no different. Keep the following in mind:

- **Ask the question, "How much risk does the business face?"** Instead of focusing first on security measures, figure out how damaging a data breach could be to your company's reputation or bottom line. Obviously, a credit monitoring service like Equifax faces enormous risk if they lose data, but even small businesses could be in serious danger if they lose customer information. In fact, small businesses may need to worry even more, as they can be easier targets for hackers (especially via automated attacks). To top it off, they may lack the financial cushion to protect them from the repercussions of a breach. By having a serious conversation about risk, executives and other stakeholders can see—and viscerally know—what's at stake, making them more likely to take security seriously.

- **Set security metrics—and watch them like a hawk.** Setting security metrics not only demonstrates the value of your security work, but it also provides a health check on your security and points out areas for improvement. For example, tracking the percentage of programs without the latest security patches will alert you to potential security holes. Tracking this metric could have prevented the Equifax breach as well as WannaCry, as both breaches attacked vulnerabilities that had patches released months earlier[2,3].
- **Strong security comes from proper management.** To build on the previous point, measuring key indicators in the environment allows you to improve your processes. As they say, "What gets measured gets managed." For example, measuring how quickly your team responds to security incidents can let you know if you need to improve processes in any way, helping you provide better services to your organization.

2. UNDERSTAND THE ENVIRONMENT AND DEFINE THE "CROWN JEWELS"

If you've ever watched heist movies, you know robbers are always after some big score. In Ocean's Eleven[4], they're looking to rob three casinos. In other movies, they're looking to rob banks. And in the BBC® series Sherlock[5], Moriarty robs the crown jewels (and purposely gets caught).

If you've ever watched heist movies, you know robbers are always after some big score.

In each of these situations, the victims guard these prizes with incredible security. When it comes to protecting your customers, you need to know what the "crown jewels" are within their environment so you can keep out the Moriartys.

You likely already have a plan for maintaining and protecting key servers or critical endpoints. Now, you need to look at the "jewels" within them. And as the IT professional in house, you already know the lay of the land, helping you "case the network" the way a cybercriminal would.

To start, define your crown applications, crown systems, and crown data. Additionally, you need to discover who your crown employees are. Once you do, put processes in place to protect them.

In many cases, if a certain individual is compromised, the company could be devastated. Imagine what would happen if a chief financial officer's laptop was compromised—that could certainly cause a major problem for the company.

Other times, it could be a crown process or access point. For example, in the case of the Target® data breach, the system vulnerability came through their third-party HVAC vendor[6]!

In other cases, you should focus on crown data. For example, health records contain an incredible amount of sensitive data, which can often lead to a lucrative payday for cybercriminals. Credit information can also be enticing to many hackers.

Credit information can also be enticing to many hackers.

In short, companies should define their crown jewels and heighten their security around these items. Additionally, companies should regularly review their security policies for these items—whether they're important individuals, systems, access points, or data. While it's impossible to secure everything, defining and protecting a company's crown jewels should be the top priority for anyone providing cybersecurity.

3. IMPLEMENT GOOD CYBERHYGIENE

So far, we've focused on shifting the conversations with your customers from security to risk. But the fundamental rules of cybersecurity still apply—you need the right technology, the right processes, and the right effort to improve security and reduce risk.

You still must practice good cyberhygiene. Remaining vigilant about security maintenance can prevent potential disasters. Often, the simplest attacks succeed, like a phishing attack or a malicious email download.

So make sure to do the following:

- **Put strong antivirus on every endpoint (and make sure it runs frequently)**
- **Understand your company's data maps to keep information from falling into the wrong hands**
- **Frequently check admin rights and permissions to sensitive data**
- **Patch all systems and software regularly (and keep up with security bulletins)**
- **Implement a strong backup and business continuity plan**
- **Stay vigilant against spam—including putting technical safeguards in place on your mail servers**
- **Reduce the potential attack surface wherever possible by cordoning some machines off from the web or using virtual machines where possible**
- **Set up incident response and remediation plans ahead of time, so you have a clear playbook to work with when catastrophe strikes**

Perhaps most importantly, realize there's simply no silver bullet. It takes consistent effort and vigilance.

4. SECURE THE ENVIRONMENT AT DIFFERENT LEVELS

There's simply no such thing as foolproof security. And as you likely already know, there's no one-size-fits-all approach.

There's simply no such thing as foolproof security.

Instead, you should aim for making the wisest investments with your leadership team. You don't want to ask for too much—as executive sponsors may feel sticker shock and question the value of these initiatives. However, you don't want to miss the mark and leave them unprepared for potential breaches.

Take this on a case-by-case basis—ask the leadership team what they consider to be the company's "crown jewels," and work with them to determine the best level of security considering worst case scenarios. It may take some time and education to explain the need for practicing good, basic cyberhygiene as well as strong security awareness programs. Have this conversation with your leadership team early and often, so you can set expectations and determine the best course of action for the company.

Provide proactive, periodic updates to your leadership team. You should constantly look to how you can demonstrate your value—and keep your stakeholders reassured they are in good hands. Revisiting the level of security every quarter or semi-annually may be worthwhile to help executives stay prepared for potential threats. This is absolutely crucial for keeping up with the ever-evolving security landscape. Think about it—just a few years ago, ransomware wasn't even a major issue. Now, ransomware seems to be the weapon of choice for many cybercriminals.

5. POSITION STRONG SECURITY AS A DIFFERENTIATOR FOR YOUR COMPANY

In a world of never-ending threats, security can make the difference for both you and your entire organization.

Revisiting the level of security every quarter or semi-annually may be worthwhile to help executives stay prepared for potential threats.

The benefit to your business may seem obvious. When you provide strong security, you stand out from competitors that focus on simple maintenance services and monitoring. You also meet an obvious demand for security and boost your credibility.

What might seem less obvious is how companies can use security to their benefit. Imagine, for example, if you were working for a manufacturer that sold to public utilities. Having a strong security proposition could help that customer secure more contracts. Some companies operate in an industry where security could make or break their business—financial institutions, healthcare organizations, pharmaceutical companies, national security contractors, and public utilities, to name a few. Demonstrating constant vigilance and advanced security techniques can help those businesses compete in the marketplace.

Even if your company isn't in a regulated industry, security could still be a selling point for them. For example, imagine a company that creates smart thermostats. Their devices could be hacked and held for ransom, as some hackers demonstrated at a 2016 security conference[7]. While these attacks haven't happened yet, you could show your company how important it is to be prepared for the possibility. In fact, any Internet of Things (IoT) device poses a risk for organizations. The more you can show how these technology decisions impact risk and compliance, the more your executive team will rely on you for valuable decisions on technology implementations in the future.

Even if your company isn't in a regulated industry, security could still be a selling point for them.

6. REALIZE THAT REGULATIONS ARE YOUR FRIENDS

When a new regulation appears on the scene, most recently the EU General Data Protection Regulation (GDPR), many in the IT industry (and the IT press) struggle to understand its potential implications. Often, panic and confusion ensue.

Yet, many times, these regulations present new opportunities for IT teams who stay ahead of the curve (and present strong benefits for the people whose data must be protected). Keep the following in mind:

- **Realize regulation drives security.** With additional requirements from GDPR or even from older regulations like the Health Insurance Portability and Accountability Act (HIPAA), businesses have been forced to incorporate better security. By following the regulations, you not only get your leadership team to take security seriously, you also have guidelines to reduce potential data breaches (from the regulations, but also from the IT press as they offer educational resources to help you improve compliance).
- **Work closely with your legal, audit, and compliance teams.** In addition to your own company's regulatory drivers, you may also need to consider outside businesses or partnerships that connect with your company for regulatory drivers. These requirements may incur auditing, monitoring, and other reporting responsibilities that will need to be implemented (in terms of technology and process). Open and frequent communication with colleagues in legal, auditing, and compliance will help ensure everyone's on the same page and help avoid any needless emergencies.
- **Privacy regulations are growing.** With GDPR, the scope of privacy regulations has greatly expanded. Now, organizations operating outside of the EU must comply with the regulation if they come in contact with the personal data of EU citizens. Expect this to be a sign of things to come—expanded scope and greater emphasis on data privacy.

Security regulations really are your friends. They improve the security not just of individual organizations, but for everyone (which is important for the interconnected nature of the web). And as an IT professional, feel free to leverage these regulatory drivers to get management's attention and support for your security program initiatives.

7. BOOST YOUR SECURITY KNOW-HOW

As we mentioned before, the cybersecurity field changes all the time. It wasn't too long ago that on-premises backup was enough for helping people recover data; now, you almost need an additional cloud-based copy since some malware strains specifically target backup files.

The key is to consistently update your organization's knowledge about security—both for your specific users and for the industry in general. Here are a few key tips:

The key is to consistently update your organization's knowledge about security—both for your specific customers and for the industry in general.

- **Create a knowledge base in your organization.** First, you want to ensure your organization has the information and skills it needs to properly serve its employees, partners, and clients. Everyone in your organization should be trained on the basics—such as the fundamentals of monitoring, access controls, credentials, and proper cyberhygiene. As you work with employees on how to be good security stewards, they will learn to make good decisions (e.g., spotting and avoiding social engineering scams) and be part of the solution when problems arise. But make sure they share critical information, like configurations to a central repository (e.g., a knowledge base), so the organization doesn't lose valuable data that can support incident response and security investigations.
- **Stay on top of current events.** Staying ahead of the curve requires a lot of research and reading. Start by skimming daily articles and resources from a few key outlets. If you find a resource you like, sign up for their newsletter or blog. Here are a few good recommendations:
  - The United States Computer Emergency Readiness Team: https://www.us-cert.gov
  - SANS.org (which has newsletters and blogs): https://www.sans.org
  - The Cloud Security Alliance: https://cloudsecurityalliance.org
  - ZDnet: http://www.zdnet.com
  - Dark Reading: https://www.darkreading.com
  - CSO Magazine: https://www.csoonline.com
- **Consider certifications.** Certifications can help your employees stay on top of the latest trends and provide frameworks to combat the bad guys. Beyond

that, certifications can be an excellent marketing tool, lending credibility to your business. In particular, look at getting the Certified Information Security Services Professional (CISSP) certification, the Certified Ethical Hacker (CEH) certification, or the International Information System Security Certificate Consortium (ISC)2 certification.

» **Get involved with communities.** It also helps to get to know other information security professionals. Consider joining ISACA and gaining certifications through them. Additionally, there are likely several conferences in your area that occur each year. For example, some of the big names include the RSA Conference, the Black Hat Conference, the DEFCON Hacking Conference, Cloud Security Expo, and Cybersecurity Europe, just to name a few.

8. BUILD A CULTURE OF SECURITY

Security must be part of the DNA of nearly every organization. Technology, while helpful, can only take you so far. With new strains of malware, malicious websites, and sophisticated phishing emails coming online every day, technology can only catch up so much.

That's why it's important to offer regular security training for your employees (and perhaps your partners and clients). Teaching them good security habits—like changing passwords frequently, using different credentials for each service (perhaps using a password tracker), and turning on device encryption on their mobile devices—will protect not only your business but also them. And regular means just that—it shouldn't be a one-time deal. Provide refresher trainings as often as possible.

You should also send regular security updates to your users, partners, and perhaps even your clients (especially when there's a major attack).

You should also send regular security updates to your users, partners, and perhaps even your clients (especially when there's a major attack). For example, the Google® Docs attack from 2017, while sophisticated, used a phishing email that tricked users into providing their Google credentials to a false website. From there, the hackers could gain access to that person's account and contacts, allowing them to repeat the process with victim's friends and colleagues. A simple email warning from your organization to its employees stating not to open an email when a major attack occurs can save you a lot of grief.

9. USE SECURITY TO OPEN DOORS FOR YOUR INITIATIVES

Cybersecurity will likely always be an ever-present need in the marketplace. By positioning your IT team as focused on meeting security challenges (and keeping up with trends using the steps mentioned before), you'll have a path to finding executive sponsorship.

Security can pave the way for other important benefits for your teams. For example, you could strike up conversations that begin with talks about layered security, but then use it to convince executive sponsors of the value of a holistically well-managed environment. You may hook them with security, but what about improving network performance or backing up key documents in the event someone accidentally deletes a file? Once you've started talking to executives about security investments, remember to consider peripheral benefits that may be of interest to them (e.g., a security monitoring tool, which also identifies the significant network resources abused by employees live streaming NBA or NFL games over the company network).

Staying in touch with a larger community of security experts will help you stay on the cutting edge in the fight against the bad guys.

10. FIND ALLIES IN THE FIGHT AGAINST CYBERCRIMINALS

Cybercriminals have their own communities. They learn their trade on both the web and the dark web.

It's important to find your own allies in this fight. Whether by joining professional organizations, going to meetups or conferences, or by reading articles online and sharing them—staying in touch with a larger community of security experts will help you stay on the cutting edge in the fight against the bad guys.

Don't limit yourself to cybersecurity communities—attending nearly any gathering for IT professionals can yield benefits for you. For example, attending a sales training might teach you how to better position security in the context of IT. It may help you learn how to position risk better as well, earning you more credibility inside the business.

You don't have to fight the bad guys alone.

THE OPPORTUNITY IN FRONT OF YOU

The changing cybersecurity landscape offers tremendous opportunity for you to grow your career. Your ability to translate security in terms the business will understand will unlock this opportunity.

Just remember to keep these security tips in mind—focus on risk, make wise investments, practice proper cyberhygiene, and stay on top of the trends and changes. By doing that, you'll stay proactive in the fight against the cybercriminals and end up with happy executives, users, and fellow IT team members.

REFERENCES

[1,2] "Equifax Officially Has No Excuse," Wired. https://www.wired.com/story/equifax-breach-no-excuse (Accessed December 2017).

[3] "The 'WannaCry' Ransomware Attack Could Have Been Prevented. Here's What Businesses Need to Know," CNBC. https://www.cnbc.com/2017/05/17/the-wannacry-ransomware-attack-what-businesses-need-to-know-commentary.html (Accessed December 2017).

[4] "Ocean's Eleven," Warner Bros. Pictures. December 2001.

[5] "Sherlock," BBC One. July 2010.

[6] "Target Hackers Broke in Via HVAC Company," Krebs on Security. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company (Accessed December 2017).

[7] "#DefCon: Thermostat Control Hacked to Host Ransomware," Infosecurity Magazine. https://www.infosecurity-magazine.com/news/defcon-thermostat-control-hacked (Accessed December 2017).

[8] "Path to MSSP," SolarWinds MSP. http://pages.solarwindsmsp.com/path-to-mssp-wp-ungated.html (Accessed December 2017).

SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premise, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals – IT operations professionals, DevOps professionals and managed service providers (MSPs) – to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.

© 2018 SolarWinds Worldwide, LLC. All rights reserved.

The SolarWinds, SolarWinds & Design, Orion, and Thwack trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.