## Table of Contents

Introduction .................................................................................1

Top 6 ways to detect and respond to security threats .......................2

Build better ‘apptitude’ with these 4 application security tips ..........5

Your mobile device security checklist ...........................................7

The importance of risk management training ..................................10

How to build a cyberthreat hunting team with a small security team ..12
Introduction

The aim of this guide is to raise awareness about the most common cyber risks and threats facing individuals and organizations in 21st century daily life and to provide helpful tips and strategies for addressing them.
Top 6 ways to detect and respond to security threats

In September, more than 500 million Yahoo! customer accounts were found to have been compromised, marking one of the largest data breaches on record. Astoundingly, the initial infiltration took place in 2014, meaning two years passed before Yahoo! caught wind of the intrusion. What’s more, it took an additional two months for the internet media giant to disclose the breach, and their inadequate response clearly left much to be desired.

If nothing else, the event serves as an example of how challenging threat detection and response is even for large companies. Let’s look at some of the top ways to detect and respond to cyberthreats in your organization.

Detection

1. **24/7/365 Real-time monitoring:** Cybercrime never sleeps, and neither can your organization’s threat detection strategy. Up-to-the-second details about activity on your network are the only way that threats can be caught before they cause serious damage. After all, it only takes three seconds for many forms of ransomware to start encrypting data once downloaded. It’s vital, then, that your organization has a network monitoring tool or service in place to identify threats the moment they arise.

2. **Threat analysis:** The problem that traditional SIEM network monitoring tools such as security information and event management pose is their inability to sift out false positives effectively. To really be able to tell the sheep from the wolves, it’s important to use a combination of analytics and human expertise.

3. **Automatic alerting:** Every organization needs to establish a framework that ensures the appropriate stakeholders are notified immediately when threats are of a certain caliber or level of progression. The sooner the right people are notified of an incident, the more swiftly and efficiently they can respond to it.
Response

1. **Create an incident response plan:** Quick thinking is vital in any cyberthreat scenario, but no amount of reflexiveness compares with preparedness. Organizations must assign response roles to department heads, managers and, to an extent, even the lines of business. Each individual in a company needs to know what his or her role is in responding to a cyberthreat, and this demands that they be educated on these protocols ahead of time.

2. **Remediate the threat:** An organization’s first priority should be to contain the current threat. If there has been a data breach, pinpoint the source of exfiltration and plug it. If ransomware or other malware has gotten onto the network, quarantine the affected systems. These responses should not be knee-jerk reactions, but rather, the application of a premeditated course of action. Just like a slow response can result in greater damage, rash or desperate reactions reduce the likelihood of a swift, smooth remediation.

3. **Employ damage control:** Some threats are nipped in the bud without any casualties. Others, however, will incur damages that need to be addressed right away. It’s important that an organization’s chief information security officer or other predesignated IT manager inform the CEO of any losses. From here, the CEO can then update other stakeholders tactfully, and in such a way that will not incite alarm, but will instead quell the most immediate concerns. Doing so successfully will require anticipation of what these concerns might consist of, and a discussion for how they can be best addressed.
Creating a culture of cybersecurity awareness

Accomplishing all of the recommended actions by relying solely on in-house expertise is much easier said than done, which is why so many mid-market organizations are now turning to managed detection and response (MDR) services. Unlike the security information and event management (SIEM) software of old, MDR provides a security operations center that is supported by the knowledge and expertise of dedicated security engineers. These professionals use a combination of analytics and qualitative cybersecurity assessments to enhance your organization’s overall detection and response strategy, and ultimately cultivate a culture of cybersecurity awareness.
Build better ‘apptitude’ with these 4 application security tips

Under the banner of “Our Continuously Connected Lives: What’s Your ‘Apptitude’?” we’ll walk you through some of the best ways that you can enhance your organization’s application security.

1. Vulnerability scanning

As cyberattackers become better at exploiting weaknesses in company networks, frequent vulnerability scans and overall security assessments will be pivotal to identifying application security deficiencies. According to TechTarget, these scanners usually function by cross-referencing databases that contain “known security holes in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts.” From here, simulations will attempt to test these attack paths to get a strong sense for what’s at stake. While it’s true that you can’t necessarily preempt every cyberthreat, it’s important to continually assess your defensive security posture by seeking out flaws in your applications and network infrastructure.

2. Updating software

Whether you’re running third-party applications or proprietary software, the importance of security patching cannot be overstated. For proprietary solutions, new script vulnerabilities will need to be addressed quickly and efficiently. For vendor-bought solutions, new critical updates should be applied sooner rather than later. Earlier this year, for example, Microsoft added features to its Office suite of products that would help prevent malicious macros, which hide ransomware and other nasty threats, from executing. Delay these types of updates, and you risk leaving yourself open to attack.

What’s more, many security patches are delivered after a developer finds security flaws in the program’s code, not necessarily in response to a hack. The problem is that cybercriminals pay attention to these updates, because they can act as a tip-off for security holes. In brief, the sooner and more frequently you patch your applications, the better.

Sometimes a well-timed update is the only thing standing between your business and downtime.
3. Managing devices

One of the most significant threats to an organization is the downloading and installation of malicious applications that could put company data at risk. To prevent this, IT admins need to make sure they have a device management strategy in place. One of the best ways to achieve this is through the deployment of an application control tool that gives admins the ability to blacklist suspicious software, whitelist legitimate applications and vet new programs that employees may attempt to install on company machines. Likewise, mobile device management tools will be important for securing smartphones that are on the network.

4. Creating best-practice polices

Arguably the most important item on this list, and the piece of advice that is most central to closing security gaps in general, is to create best-practice policies that explicitly include application usage. These should outline security standards for applications that mandate secure communication backed up by encryption, password protection and limited access (within reason) to personally identifiable information and other sensitive data. These policies should also require that the most up-to-date software be used at all times. In the event of a zero-day exploit, or perhaps a breach of a third-party application vendor, IT and the lines of business need to have a strong plan of action in place to limit that app’s access to sensitive data, and prevents its use.

You can’t necessarily prevent bad things from happening, but if you take these four steps, you can certainly improve your “apptitude.”

To read more about how to better secure your infrastructure, click here.
Your mobile device security checklist

From government agencies to financial institutions, the inclusion of mobile devices in business operations is raising a long list of concerns including the threat of lost or stolen devices, shadow IT, connections to non-secure networks and more.

“Networks are inclusive of everything from smartphones to smartwatches and beyond.”

However, mobility isn’t a trend that businesses and users are ready or willing to shy away from. The opportunities for return on investment are too substantial to start backpedaling now. Hospitals are using tablets and smartphones to take notes and access patient medical records as they move between wings of a facility, or to remotely track out-patient vitals. Banks and credit unions are starting to offer customers mobile applications that make banking more convenient. Not to mention, new reports suggest that many industries will soon add wearable technology to their arsenal of mobile devices.

Keeping track of mobile and remote endpoints was hard enough when we were just dealing with laptops. Now, business networks are inclusive of everything from smartphones to smartwatches and beyond.
Mobile cybersecurity: A checklist

Naturally, mobile endpoint security is a complicated endeavor since there are literally so many moving parts involved. However, there are a few overarching checklist items that organizations must consider as they attempt to mitigate risks associated with mobile devices. Let's take a look:

1. Layout clear company policies for mobile: Whether you're allowing bring your own device or you're distributing corporate-owned, personally-enabled devices, it's vital that any mobile endpoint that will be used for work purposes adhere to a well-defined set of boundaries. These need to be official, enforced and implemented across all departments of your organization. End-user awareness is the best defense against targeted threats such as phishing schemes, and it can abate careless user activity.

2. Know what endpoints are accessing your network: This is vital to not only ensuring that your employees are adhering to best mobile practices, but also to being able to detect anomalous behavior — be it within the organization, or at the consumer level (i.e., unusual mobile banking activity). At the end of the day, every interaction that a mobile device has with your network is logged and recorded. It's really just a matter of knowing how to identify suspicious or unusual activity.

3. Deploy a mobile management solution: To be fair, there are countless mobile security solutions, and enough initialisms (MDM, EMM, MAM, IAM, etc.) representing them to give your CISO or CIO a pounding headache. That said, having a methodology in place to remotely protect lost or stolen endpoints is a vital aspect of incident response. You need to have an awareness of what mobile management solutions are out there, and which ones are necessary to respond to threats in your unique mobile environment.
Are you ready to protect your mobile IT environment?

With so many different types of mobile devices connecting to your network from such a vast array of locations, checking off all three of the recommended actions is a lot easier said than done. There are so many intricacies involved in developing mobile policies, and so many people who have to be included in that process. Threat detection in such a dynamic endpoint ecosystem is sort of like trying to pick misshapen snowflakes out of a blizzard. And with so many different mobile security offerings at play, it’s not always easy for IT managers to make the best use of the funding available to them as they attempt to secure the network.

The best advice we could give you here is this: Don’t try to do it all by yourself. Work with a cybersecurity partner capable of helping you answer this question: “Am I safe?”
The importance of risk management training

PricewaterhouseCoopers recently released its 19th annual CEO survey, and this year, the board room listed cybersecurity among its most pressing concerns. This isn’t shocking considering the immense amount of damage cyberthreats have caused in the past 12 months. We’ve witnessed cyberattacks on the power grid, digital bank heists of historic proportions, hospitals being held hostage by ransomware and other horrific attacks that seem to have been lifted from the pages of science fiction. Far and wide, business decision-makers are asking themselves this key question: What can we do to better protect our assets?

The marriage of cybersecurity and risk management

In a separate survey, PWC found that 91 percent of organizations now follow a risk-based cybersecurity framework. This statistic is truly indicative of just how imposing cyberthreats have become to business assets.

While viewing cyberthreats less as an IT issue and more as a business concern is certainly a step in the right direction, the next move is to create a risk management strategy that’s inclusive of the entire organization – or as the architects of NCSAM put it, “From the Break Room to the Boardroom.” For the sake of remote workers who have a laissez-faire definition of the home office, we might even add the bedroom.

There is no room in an organization that is above cybersecurity best practices.
Education is the great equalizer

The important thing to understand about cyberthreat-related risk is that no one is immune. The C-suite is in just as much danger from phishing schemes that aim to implant ransomware and other cyberthreats on the network as the lines of business. In some ways, the high level of privileged access given to upper management puts them at greater risk of making a mistake.

“Every facet of an organization needs to be well-educated on the many sources of cyber risk.”

Long story short, every facet of an organization needs to be well-educated on the many sources of cyber risk. This goes beyond just laying out workflow protocols that attempt to mitigate risk all at once. To truly improve cybersecurity, business leaders need to work with their IT managers to actively educate the lines of business – as well as fellow board members – about the types of actions that put an organization’s data at risk. This includes instilling cybersecurity best practices into employees, contractors and vendors but also keeping them up-to-date on the most recent threats.

One approach that can help yield results is to have monthly meetings or training sessions that bring colleagues, regardless of their rank, up to speed on the newest tactics being employed by hackers. A weekly email blast highlighting the newest schemes can prevent workers from being blindsided by the more clever schemes (one type of ransomware called PETYA spreads in fake job applicant emails sent to unsuspecting human resources departments).

For those organizations that need help developing a template for risk management training, there are plenty of third-party organizations that are dedicated to enhancing cybersecurity awareness, and making the virtual world a safer place, one business at a time. To learn more, contact Arctic Wolf Networks today.
How to build a cyberthreat hunting team with a small security team

In light of several attacks on critical infrastructure (one involving ransomware in Michigan, and another in Ukraine that resulted in a power outage for 225,000 people), it's clear that having a strong security posture will be more important than ever for utilities and energy companies in the coming years.

One of the most important places to start in this endeavor is with cyberthreat detection, and more specifically, cyberthreat hunting.

What is cyberthreat hunting?

On a superficial level, hunting is exactly what it sounds like: a proactive search for cyberthreats in your organization's network. But upon closer examination, we learn that there is a lot to this feat.

According to DarkReading contributor David J. Bianco, “hunting is not an automated process.” In fact, it requires a concerted effort that's backed up by a strong understanding of the cyberthreat landscape and security infrastructure.

“A savvy hunter understands that the attackers can accomplish their goals in many ways and examines the data from several viewpoints to compensate,” Bianco wrote.

What’s more, hunting isn't like penetration testing. Pen tests are certainly part of the equation; however, these assessments aren't usually 24/7 endeavors, and hacking is.

The hunt, on the other hand, never ends – or at least it shouldn't. This is especially true in critical infrastructure, where monthly, weekly and even daily penetration tests just aren't enough when so much is at stake.
Challenges, solutions and rewards of hunting

Many organizations struggle with hunting for the simple reason that they have small security teams, or at least a security team that isn’t capable of supplying the 24/7/365 threat-seeking capabilities that are necessary for protecting something as important as critical infrastructure. The fact is, managing SIEM the right way requires, as Bianco has illustrated, proactive application of human security expertise. Data analytics certainly plays a big role in this endeavor, and it helps weed out threats, but a human hand at the helm is just as important.

So what are your options? Bringing on an entirely new security team and investing in SIEM isn’t exactly economical. You could outsource everything to a security operation center, but that’s not ideal for organizations that need to be actively included in these endeavors.

Interestingly, this isn’t an issue that’s unique to critical infrastructure. Health care, finance, law and other compliant industries need to at least have a finger on the trigger, so to speak. This requirement has led to the growth of an entirely new market in recent months called managed detection and response (MDR). The benefit that MDR has over SIEM, SOC and MSSPs is that it supplies “hunting” experts to clients who can manage a SOC, but who also work directly with your internal security team to make sure they’re still the ones calling the shots.

So, in a lot of ways, MDR acts as a spotter in your cyberthreat hunting endeavors – and for assets as essential as critical infrastructure, that goes a long way.

To learn more about MDR, click here.
To learn more about cultivating a culture of cybersecurity awareness in your organization, go to www.arcticwolf.com