2018

Top 7 Cybersecurity Challenges in 2018

ACTION1 CORPORATION

www.action1.com

1. Action1 Research: Top 7 Cybersecurity Challenges in 2018

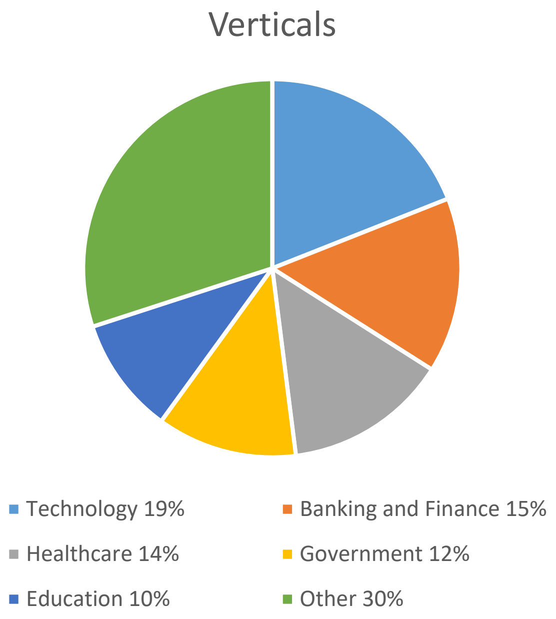
1.1 Introduction

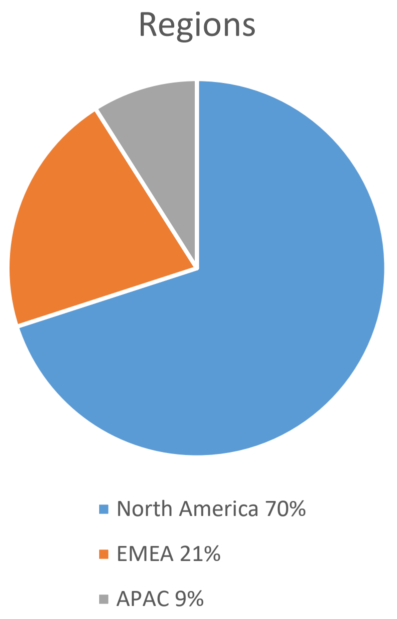
This report highlights the results of a study of what cybersecurity professionals perceive as their main challenges; which types of threats they are mostly concerned about, based on their experience; what plans do they have to solve these challenges. The purpose of this report is to determine typical successes and failures various organizations have and provide guidance to cyber security professionals to improve their practices in IT security management.

The data for this study was collected in July 2018. Respondents were cybersecurity professionals with different titles. They were asked to share their views on different aspects of endpoint security via a survey. The survey questions allowed one or multiple responses. We thank all the respondents for sharing their insights!

1.2 Survey Demographics

Participated 521 organizations: 125 large enterprises (24%) and 396 SMB (76%).





Challenge #1: Employee Cybersecurity Skills

Survey Responses:

- 81% of respondents included this among their top challenges
- 21% of respondents said this as their #1 priority

Lack of cybersecurity education among organizations’ non-IT employees substantially increases risk of phishing attacks and introduces many other issues related to employee negligence.

Some common examples include:

- Employees use one “favorite” password for all of their services.
- The passwords they pick are usually too simple and basic.
- Most people are still prone to phishing attacks via email and phone, even at the top of organizations.
- Thinking that it’s IT department’s job to secure everything and thus neglecting their cybersecurity duties, such as negligent access right assignments by data owners, failure to lock their computers when away from the desk etc.
- It’s noteworthy that with ongoing digital transformation most of these issues now also affect traditional “blue-collar” industries, not just office-based environments.

Recommendations:

- Companies like CompTIA offer basic cybersecurity training for non-IT employees, which is something organizations should to consider.
- IT departments can also consider creating their own simplified “Cybersecurity 101” courses internally in collaboration with their HR departments to implement it in addition to their standard training and employee onboarding procedures (such as sexual harassment and safety).

Challenge #2: Continued Evolution of Ransomware

Survey Responses:

- 75% of respondents included this among their top challenges
- 25% of respondents said this as their #1 priority

This remains a huge concern as a never-ending series of evolving ransomware and new ransoms paid by major organization continue to dominate the news. WannaCry, Petya, NotPetya, CryptoLocker, Locky, CrySis, Bad Rabbit – and many other types of ransomware with weird names continue to cause financial and reputational losses. And Shadow Brokers only make things worse by offering an illegal marketplace for criminals to buy "ammunition" or even turn-key "ransomware-as-a-service" solutions for sophisticated cyberattacks.

Recommendations:

- Organizations need to continuously review their user right assignments and permissions to all kinds of data and follow the "need-to-know" (also known as "Least privilege") methodology to their data and IT infrastructure.
- Automated detection of ransomware is now supported by many antimalware products. Organization shall re-evaluate the cybersecurity systems they use to better understand their capabilities and how effective they are in preventing ransomware or minimizing damage caused by it. **Tip**: Ask your cybersecurity vendor about their ability to detect and prevent ransomware and what kinds of ransomware do they support.
- Organizations shall backup sensitive servers and endpoints regularly in order to have a restore capability in case crypto-ransomware maliciously encrypts important files. File storage systems with automatic versioning and rollback capabilities should be considered as well as a viable and efficient alternative to traditional backup and recovery systems.

Challenge #3: Patching and System Hygiene

Survey Responses:

- 67% of respondents included this among their top challenges
- 17% of respondents said this as their #1 priority

Sounds like a throwback, yeah? But unfortunately patching still remains a great challenge for so many organizations and constant thoughts about Patch Tuesday keep a lot of system administrators awake at night.

Recommendation:

Organizations need to re-evaluate their current patching systems and procedures in place and define the steps needed to establish the right practices.

Challenge #4: Unmanaged Devices

Survey Responses:

- 62% of respondents included this among their top challenges
- 5% of respondents said this as their #1 priority

Do you think that problem is solved once your brand-new cybersecurity system is deployed across your entire network? Think again. Does your system automatically detect new endpoints in the network, such as new laptops or phones your employees bring to work? Or a field rep losing their laptop while on a trip, buying a new one and connecting to your network from an airport? According to the survey responses, such situations happen regularly and the issue remains one of the top concerns for a lot of organizations.

Recommendation:

Test your cybersecurity solution and ask its vendor how their product deals with unmanaged devices on your corporate network. How frequently your network is scanned for new devices? What happens when a new device is discovered? Is protection of new devices enabled automatically? How many devices do I have in total on my network and how many are not being managed and adequately protected? (is there a report or even a real-time dashboard showing that?)

Challenge #5: Integration of Cybersecurity Tools

Survey Responses:

- 47% of respondents included this among their top challenges
- 10% of respondents said this as their #1 priority

No technology is 100% perfect and self-sufficient. This is where integration and vendor eco-systems come into play. SIEM, threat intelligence feeds, next gen firewalls, IT helpdesk services, malware sandboxing systems, analytics tools and more. They can all greatly complement each other if properly integrated. In reality, this is easier said than done as systems constantly evolve and change their APIs, sometimes without proper notice, as indicated by some of the survey respondents.

Recommendation:

Ask your system vendors about their integration maintenance policies and availability and cost of professional services to implement new integrations. Connect with the fellow users of the same systems (ask your vendor for references or use vendor’s online customer community or live conferences) and exchange experience with different integrations.

Challenge #6: False Positives

Survey Responses:

- 42% of respondents included this among their top challenges
- 18% of respondents said this as their #1 priority

With all the sophistication of modern IT security solutions, the challenge of fine-tuning them per organization-specific needs remains important. As quite a few recent successful cyberattacks have shown, the problem of finding a needle (a real attack indicator) in the haystack of false positives makes such attacks very possible. IT security teams are getting overwhelmed by all kinds of alerts generated by their systems and chances of missing what really matters are very high.

Recommendation:

Some of the newest technologies that utilize artificial intelligence (AI) and machine learning (ML) are capable of weeding out a lot of false positives. Even some older rule-based systems, if configured diligently, can serve the purpose. However, there is a risk of losing critical pieces of information because of incorrect configuration or lack of sufficient “training” of such systems as it pertains to system’s machine learning capabilities, which can result in “false-true” positives (such as a real attack indicator being automatically suppressed as non-important by mistake). **Tip**: Ask your cybersecurity vendor about their automatic threat classification capabilities and what technologies are being used (AI, ML or simple rule-based?)

Challenge #7: Automatic Remediation

Survey Responses:

- 30% of respondents included this among their top challenges
- 4% of respondents said this as their #1 priority

All right, your system spotted a cyberattack. What now? What if it originates from China during their waking hours while your entire IT staff is having a good night sleep? The ability to tackle new issues automatically (or semi-automatically) can come very handy in such situations. Kill a process that encrypts too many files. Block a network file share if it allows excessive access. Uninstall newly installed unauthorized application. Automating such actions can help you sleep better at night.

Recommendation:

You should review your current automation capabilities and evaluate what can be further automated. You have to be cautious though, because automatic remediation without carefully defined strategy can cause major business disruption or even worse, encourage attackers to try more sophisticated ways of penetrating your network.

About the Report

This report was produced by Action1 Analyst Lab based on surveys among cybersecurity professionals around the world to highlight current industry trends and analysis of the cybersecurity landscape.

About Action1

Action1 provides a Cloud-based lightweight endpoint security platform that discovers all of your endpoints in seconds and allows you to retrieve live security information from the entire network using plain English queries, with a Google-like experience, right in your web browser.

Unlike legacy, on-premise, hard-to-scale, heavy-weight solutions that rely on costly ongoing scans of security information that quickly becomes outdated before it's even utilized, Action1 enables endpoint security and compliance that reduces threat response times from days to minutes, while not requiring costly on-premise deployment and maintenance.

For more information, please visit www.action1.com