Main Cybersecurity Challenges

Joe St Sauver, Ph.D.
M3AAWG Expert Advisor

M3AAWG 62, Toronto, Ontario

Introduction

- Cybersecurity is an ongoing challenge for most sites. Some challenges may be **general,** while other challenges may be more **specific/technical.**
- **Today we'll outline some of the main general and specific/technical challenges we see, just to get the conversation started.**
- Your organization may face different challenges. **We hope you'll contribute your perspective about any topics we don't mention.**
- We've endeavored to include **references** for any statistics we cite, since some of them are so high (or so low) as to be almost shocking.
- We've also endeavored to suggest basic approaches to mitigating some of these issues, when there is an obvious option to consider. Some challenges may be unsolved to-date.

Cybersecurity Challenges: General and Technical Outline

GENERAL	SPECIFIC/TECHNICAL
1) Cybersecurity Leadership	1) Cybersecurity Incident Response Plans
2) Inertia	2) DDoS
3) Monoculturality	3) Disaster Recovery/Business Continuity/Backups
4) Over-Complexity	4) Instrumentation of Systems and Networks
5) Reactivity	5) Multifactor Authentication
6) Threshold Effects	6) Nation-State Attacks
7) Time Horizons	7) Ransomware
8) Underinvestment	
9) Understaffing	
10) Underwriting (aka Cyber Insurance)	
11) User Privacy and Data Protection	

<u>General</u> Cybersecurity Challenges

1) Cybersecurity Leadership

- If cybersecurity isn't a priority for your organization's executives, it will be difficult to have a successful cybersecurity program. **Senior cybersecurity staff members are also aging.**

- **Example: "A Looming Crisis -- The cybersecurity industry is on the brink of a leadership vacuum.** With 34% of the workforce now aged 45-54, the sector faces an imminent challenge as senior professionals approach retirement, yet 40% of organizations still report vacancies at the senior manager or director level. [...] Organizations are struggling to build a strong leadership pipeline, which is essential for maintaining stability in an increasingly complex threat environment." [emphasis added]
  [ref: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-hidden-culture-crisis-and-human-burden-undermining-cybersecurity-resilience]

  See also "The Cybersecurity Leadership Crisis Dooming America’s Companies," https://www.forbes.com/sites/bobzukis/2024/07/26/the-cybersecurity-leadership-crisis-dooming-americas-companies/

- **Mitigation:** Succession planning? Leadership development programs?

2) Inertia (Obsolete/End-of-Life Legacy Systems Remaining In Use)

- **Risk:** Obsolete systems and software may no longer be getting **vendor security patches,** leaving those systems vulnerable to known attacks. This issue has been flagged by national cybersecurity authorities, see for example https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products

- **A Specific Looming Example:** "After October 14, 2025, Microsoft will no longer provide free software updates from Windows Update, technical assistance, or security fixes for Windows 10." [ref: https://www.microsoft.com/en-us/windows/end-of-support?r=1]

  An estimated 400 MILLION systems do not meet Windows 11 minimum requirements [ref: https://www.theregister.com/2023/10/27/microsoft_petitioned_to_keep_windows/]

- **Mitigation:** When possible, replace obsolete hardware and software outright. If that's not possible, consider shifting to currently supported operating systems/applications with lower minimum requirements (this may not always be possible, and may come with substantial training and support costs – going from Windows to Linux can be a BIG jump)

3) Monculturality

- **Risk:** If an incident occurs in a monoculture, it will often have broad impact.

- **Recent Specific Example:** July 2024 Crowdstrike update issue. Crowdstrike says that it is used by "538 Fortune 1000 companies, 298 Fortune 500 firms, and 43 of 50 U.S. state [governments]" – that's substantial market share.

  [Ref: Testimony of Adam Meyers, Senior Vice President, CrowdStrike Holdings https://homeland.house.gov/wp-content/uploads/2024/09/2024-09-24-HRG-CIP-Testimony-Meyers.pdf]

  See also "Widespread IT Outage Due to CrowdStrike Update," https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update

- **Mitigation:** Diversify when possible (but diversification requires availability of satisfactory alternatives, and sometimes options may be limited).

4) Over-Complexity Resulting in *In*security

- **Risk:** Systems and networks have become so complex that they have become impossible to fully understand and effectively secure.
- **Again, Not A New Idea!** B. Schneier, 1999, "A Plea for Simplicity: You can't secure what you don't understand," www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

  *"**Predictions***

  > *"As systems get more complex, security will get worse.*
  >
  > *"As systems become more interconnected, security will get worse. [continues]"*

- **More Recently:** "In April 2024, ThreatDown surveyed a group of 50 companies with 1-1,000 employees to take the temperature of life in IT. The results show clearly why IT teams are crying out for effective, hassle-free, and easy-to-manage security tools. In our survey group, the average company had 440 devices to manage and just three IT staff. No wonder that 68% of them told us their biggest challenge is managing limited time and resources. And those IT staff are well aware of the burden that complexity creates for them, with **78% agreeing that the more complex an IT environment is, the harder it is to secure."** https://www.threatdown.com/blog/why-complexity-has-become-a-security-issue/
- **Mitigation?** Difficult – and simplification may result in monoculturality, which is also risky.

5) Reactivity

- The typical (real) cyber security model: ~~Prevent~~ **Detect Respond** ~~Secure~~
- Cybersecurity staff face competing demands on their time: they're continually called upon to detect and react to cybersecurity incidents (leading to alert fatigue and high stress; very burnout-prone **"emergency room doctor"**-lifestyle), BUT "fighting fires" can leave cyber security saff with no time for strategic/transformative steps that might prevent incidents from occurring in the first place (or ensure that systems are fully recovered and hardened after a compromise). This is the definition of a "**Sisyphean** task" or "**hamster wheel**."
- The typical suggestion is to more effectively leverage automation – "cue the acronyms:"
  - Security Information and Event Management (**SIEM**)
  - Extended Detectionn and Response (**XDR**)
  - Security Orchestration, Automation and Response (**SOAR**)
  - ...
- Those solutions normally require an organization to be of a certain **scale and sophistication** (and have available **budget**) and may result in **increased complexity** (see previous slide).
- **Mitigation (beyond leveraging automation as noted):** difficult.

6) Threshold Effects

- **Risk:** Law enforcement agencies can't Investigate, arrest, and successfully prosecute all cybercriminals, so they tend to focus their attentions on the "worst of the worst." The unintended consequence of that is that many cyber crimes are virtually consequence-free for the cybercriminal entities perpetrating those crimes – at least as long as they are careful not to become too noteworthy or too worthy of official attention.
- In a real world analogy, "everyone speeds" on major highways, but you're more likely to get pulled over if you're doing 35 over in a brand-new bright red Ferrari rather than doing 8 over in a couple year old Toyota or Honda)
- **Example:** The likelihood that a cybercrime entity is detected and prosecuted in the U.S. is estimated to be around **0.05 percent.** [ref: https://www.weforum.org/agenda/2020/01/partnerships-are-our-best-weapon-in-the-fight-against-cybercrime-heres-why/ citing https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors]
- **Mitigation:** We need **more cyber cops (and more specialized prosecutors),** or law enforcement needs to intentionally engage in at least some enforcement activity that **reaches down to target lower tier "average" or "street level" cyber criminals.**

7) Time Horizons: We're Way Too Short-Term-Focused

- Some cybersecurity efforts take sustained time and effort, but its seems as if increasingly there's only time for **"quick win"/short-term cybersecurity projects.** (This may a manifestation of a largely-"reactive" cybersecurity posture)

- **Cybersecurity forecasts are ALSO correspondingly short term,** frequently using just a three to five years horizon (which only gets us out to 2030 or so). For example: "Cybersecurity Futures 2030: New Foundations," https://www.weforum.org/publications/cybersecurity-futures-2030-new-foundations/

- One noteworthy exception: [U.S.] Air Force Center for Strategy and Technology is explicitly focusing on 2035 and beyond. Their promo blurb: **"Welcome to 2035: The Age of Surprise,"** https://www.youtube.com/watch?v=9Xpu2QqLnHY highlights the challenges.

- **Bottom Line:** we need to to quit "staring at our skis" and get used to "looking ahead down the slope" – at least if we want to avoid cyber "trees" suddenly appearing in our path.

8) Underinvestment

- On average, organizations spend just **10% of their IT budget on cybersecurity.** [ref: https://www.senseon.io/blog/how-much-should-a-business-spend-on-cybersecurity]

- **Risk:** Failure to adequately invest in cybersecurity can results in costly potentially-avoidable incidents. Impacts will often include both internal-to-the-organization and external costs.

- **Example: May 2017 WannaCry Ransomware attack** impacting 300,000 computers in 150 countries. [ref: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack] Successfully-attacked computers were still running outdated versions of Windows (or had failed to apply available security patches). Even a basic cybersecurity program would normally have ensured current operating systems/current patch levels, right?

- **Mitigation:** Ensure adequate investment in cybersecurity.

  I'm not going to suggest a specific value, but we could certainly have a conversation about **planned cybersecurity costs** vs **the unplanned costs of mitigating cybersecurity failures**

9) Understaffing

- We've already mentioned under**funding**, but a related problem is **understaffing.**

- **Risk:** You won't have the talent you need to keep you out of trouble, or to get you back to a secure state if you do end up getting compromised.

- **Example:** "New ISACA Research: **59 Percent of Cybersecurity Teams are Understaffed**" [ref: https://www.isaca.org/about-us/newsroom/press-releases/2023/new-isaca-research-59-percent-of-cybersecurity-teams-are-understaffed]
- Sometimes the issue isn't getting approval and budget for a new position, it's actually **finding someone to fill an approved and funded cybersecurity role** (what some refer to as a cybersecurity "talent gap.") Nice discussion in: https://www.kaspersky.com/blog/portrait-of-infosec-professional-report-2024/

- **Mitigation?** Hire more people (if you can even find qualified people to hire!) Substitute automation? (that may require people to run)? Develop your own training program?

10) Underwriting (Cyber Insurance)

- Cybersecurity risks can be "avoided, mitigated, accepted or transferred."
- **Cybersecurity insurance** is one way of transferring cybersecurity risks.
- **Risk:** Without active cybersecurity insurance *(and compliance with cybersecurity insurance terms of underwriting),* unexpected (and unbudgeted!) incident costs may need to be paid directly out-of-pocket by the organization (they're effectively "self-insured").
- However, "**87% of managers surveyed state that their company is not adequately protected against cyber risks.**" [ref: https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html]
- And even those WITH active cybersecurity insurance may find their claims get rejected: "According to a 2023 report by Advisen Cyber Claims Report, a staggering **44% of cyber insurance claims are denied** because businesses simply didn’t meet all their security requirements." [ref: https://accentconsulting.com/blog/cyber-insurance-denial-why-44-of-claims-get-rejected-and-how-to-avoid-it/]
- **Mitigation:** Obtain adequate coverage and ensure all underwriting requirements are fully satisifed (or that you're happy self-insuring against cyber security-related perils)

11) User Privacy and Data Protection

- An uptick in enforcement has put teeth behind user privacy and data protection requirements. Are you at least paying attention to data protection and user privacy?

- **Examples:** "20 biggest GDPR fines so far [2024]", https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ says that

  *"As of 2024, the cumulative total of GDPR fines is now getting close to **€5 billion**, underscoring the ongoing commitment to enforcing data protection regulations and the increasing financial consequences of non-compliance."*

- **Mitigation:** Have a privacy policy and a chief privacy officer empowered to enforce it, and at a minimum, audit your data retention and usage.

Technical Cybersecurity Challenges

1) Cybersecurity Incident Handling

- When incidents (such as a cyber intrusion or malware outbreak) occur, your cybersecurity incident response plan (CSIRP) should guide your response to it.
- Unfortunately, many companies don't even have (and regularly test) a CSIRP – only **42.7%** hit that threshold (ref: https://www.spglobal.com/esg/insights/featured/special-editorial/with-cybersecurity-risks-on-the-rise-some-sectors-can-do-more-to-prepare)
- Questions to considerfor a CSIRP include:

  -- **When** do we respond to an incident? When we suspect an incident may have occured? Or do we want to wait until we're "sure" that an incident has happened?
  -- How do we evaluate the **severity** of an incident? Does incident severity impact the organization's response to the incident? (can't do "all hands on deck" for everything)
  -- What are the **specific steps** we'll normally take to recover from common incidents?
  -- **Who gets notified?** What if email is unavailable, or a key person is on the road?
  -- **How is forensic evidence collected and protected?** Is it shared with law enforcement?
  -- How are **lessons-learned extracted and shared?**
  -- What are our plans to **make people aware of the incident response plan** itself?

2) DDoS

- **Example: The Number of DDoS Attacks Is Increasing:** "F5 Labs' 2024 DDoS Attack Trends report documents a 112% rise in DDoS attacks from 2022 to 2023, with 2,127 attacks recorded in 2023. This doubling of attacks within a year further corroborates the alarming trend identified by Imperva, which revealed a staggering 111% increase in DDoS attacks in the first half of 2024 compared to the same period in 2023." [ref: https://cybermagazine.com/articles/companies-across-cyber-sphere-warn-of-surge-in-ddos-attacks]
- **Example: Delivered Attack Traffic Volumes Are Increasing:** "Since early September, Cloudflare's DDoS protection systems have been combating a month-long campaign of hyper-volumetric L3/4 DDoS attacks. Cloudflare's defenses mitigated over one hundred hyper-volumetric L3/4 DDoS attacks throughout the month, with many exceeding **2 billion packets per second (Bpps) and 3 terabits per second (Tbps).** The largest attack peaked 3.8 Tbps — the largest ever disclosed publicly by any organization." [ref: https://blog.cloudflare.com/how-cloudflare-auto-mitigated-world-record-3-8-tbps-ddos-attack/]
- Does YOUR organization have a DDoS mitigation strategy?

3) Disaster Recovery/Business Continuity/Backups

- Disasters DO occur – data center fires/floods/quakes, electrical/cooling failures, ransomware attacks, businesses failures, etc. Outages in the cloud also take place.

- **Risk:** Having a well-architected and tested/proven disaster recovery and business continuity plan (including trustworthy offsite backups) can be the difference between an organization surviving and that organization going out-of-business.

- **Examples:** "Data Center Fires: A Detailed Breakdown with 22 Examples," Oct 27, 2023, https://dgtlinfra.com/data-center-fires/

  '"Unprecedented" Google Cloud event wipes out customer account and its backups," https://arstechnica.com/gadgets/2024/05/google-cloud-accidentally-nukes-customer-account-causes-two-weeks-of-downtime/

- **Mitigation:** Develop and test a disaster recovery/business continuity plan. Have multiple generations of backups, including offline/offsite backups. Periodically test your plan.

4) Instrumentation of Systems and Networks

- You wouldn't drive a car if you couldn't see the road ahead of you through the windshield, yet many providers run with limited insight into server loads and network traffic.
- Improving the instrumentation of your infrastructure is pivotal to knowing when a problem has happened, and being able to successfully localize and mitigate that problem.
  - Have you pre-installed fiber taps throughout your network, so they're there if you need them?
  - Do you have an **intrusion detection system (IDS)**/**intrusion prevention system (IPS) deployed?**
  - Do you at least collect **netflow**? Have you built network **baselines** so you know what's atypical?
  - What about **SNMP** data? Sometimes even simple counters can readily highlight anomalies.
  - Do you forward & centrally consolidate **server logs** in a searchable platform? For example, could you tell if someone was scanning your systems, and from where?
  - Do you monitor your **authoritative name server traffic** and **recursive DNS resolvers?**
  - What about monitoring your **wide area routing**? Could you tell if someone was announcing **more specific routes** for your address space?
  - Are your monitoring solutions keeping up with 10 Gbps, 100Gbps, and even 400Gbps rates?
  - Will your monitoring survive increasingly comprehensive encryption, use of VPNs, etc.?

5) Multifactor Authentication

- It is stunning that passwords still remain in use as a sole authenticator in 2024. ALL significant systems/all privileged access, should be protected with multifactor auth at this point. In many businesses of a sufficient size, this HAS largely been accomplished, but in many smaller businesses in particular, deployment is still only just beginning.
- **The Risk:** "... if you're not using MFA, the likelihood of compromise is about 20 times higher than people who are doing MFA." [ref: https://govcyberhub.com/2023/03/15/why-the-federal-governments-lagging-mfa-adoption-rate-poses-severe-cyber-risks-to-agency-networks/]
- Another study [ref https://jumpcloud.com/blog/multi-factor-authentication-statistics]:
  - In companies with over 10,000 employees, 87% use MFA.
  - Businesses with 1,001 to 10,000 employees, 78% use MFA.
  - **Smaller companies with 26 to 100 employees, the rate drops to 34%.**
  - **In businesses with up to 25 workers, the adoption rate is even lower at 27%.**
  - Overall, only 4% use hardware MFA (remainder use software MFA, e.g., a mobile app)

6) Nation-State Attacks

- **Nation-state level attackers** may conduct influence operations online or collect cyber-espionage (nations most frequently mentioned are **China, Russia, North Korea** and **Iran** [ref: www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors])
- **The Risk:** Nation-state attackers bring a level of resources and cyber-intelligence to their craft that routinely exceeds what's available to typical non-state attackers.
- **Classic Example:** "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack," https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (attack reportedly conducted by the Russian SVR)
- The country's supply-chain is a popular target for attacks (see https://www.infosecurity-magazine.com/news/nationstate-attacks-target/ and see https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/).
- Nation states have also even been known to "go retro," leveraging things like USB sticks ("'The Weirdest Trend in Cybersecurity': Nation-States Returning to USBs", see https://www.darkreading.com/ics-ot-security/weirdest-trend-cybersecurity-nation-states-usb).
- The best mitigation of nation-state risks may be to not be a relevant nation-state target.

7) Ransomware

- We've all heard about ransomware: malware infects critical systems, exfilitrating data and encrypting files. If the ransom isn't paid (usually using some cryptocurrency), the encrypted files may be left irretrievably scrambled. Ransomware is a major current problem. (Some statistics: https://www.varonis.com/blog/ransomware-statistics)
- **Policy mitigation? Governments continue to permit victims to pay demanded ransoms.** This means that cyber criminals will continue to engage in ransomware attacks (since it continues to be a reliable way to make money). If governments outlawed the payment of ransomware, ransomware would cease to be lucrative and might potentially become less of a problem (but see pushback in "Should there be a total ban on ransomware payments?" https://securityintelligence.com/news/federal-ban-ransom-payments/)
- **Technical mitigations? Ransomware attacks could also be made irrelevant if organizations had current backups that minimized data loss.** What's you're RPO (recovery point objective)? That is, how much data would you stand to lose since your last backup? How LONG would it take you to reload your systems from backup? How much would it cost to tighten up both of those metrics? Would it be less than paying even one ransom?

Conclusion

- We've mentioned a lot of different cybersecurity challenges. Some are mundane, some are esoteric, and there many still more obscure ones we haven't even mentioned.

- What does YOUR company believe is the biggest cybersecurity challenge?

- What can M3AAWG do to help?