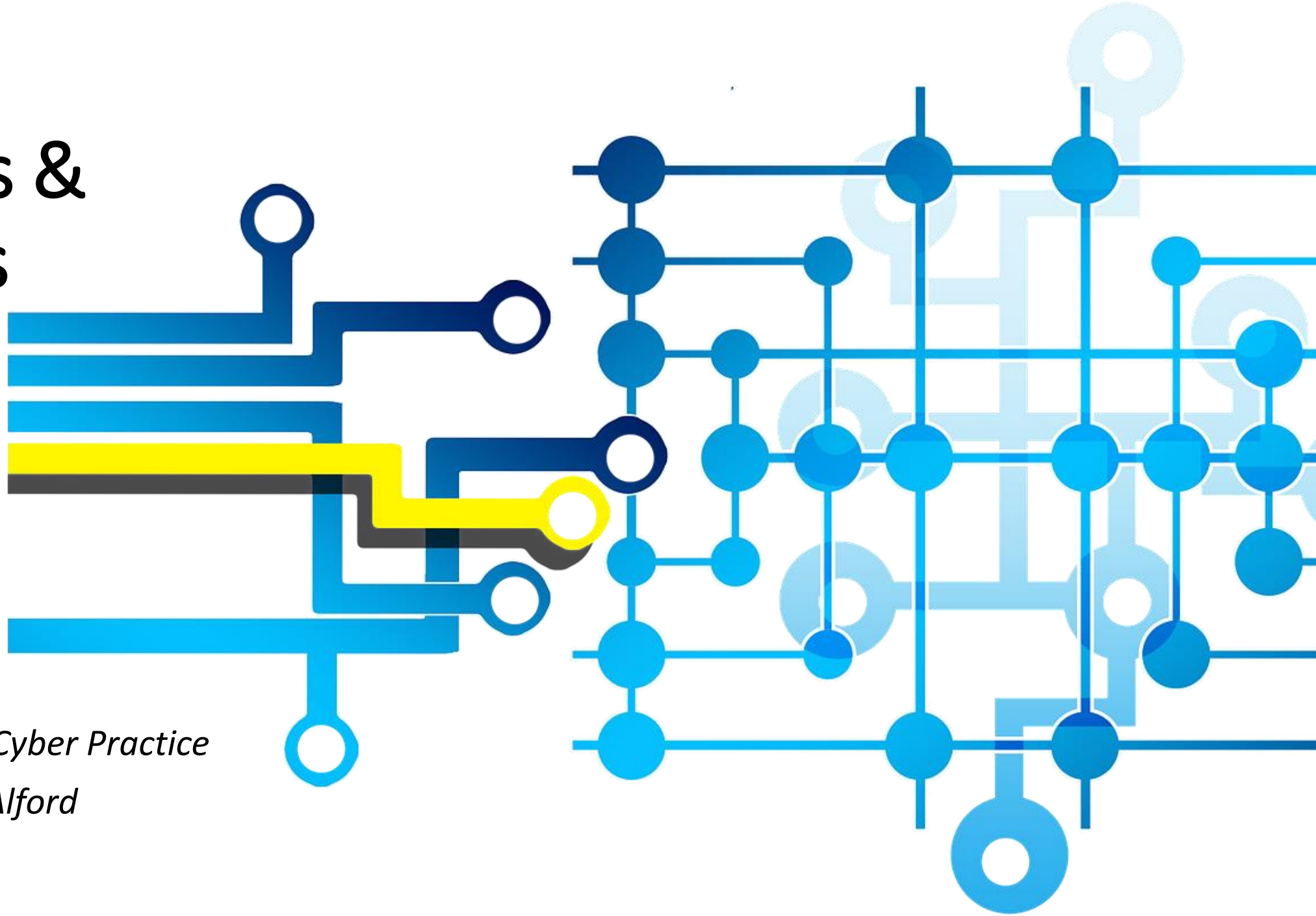
Cyber Problems & Solutions



An Overview of a Cyber Practice

By Allan Alford

Allan Allan, 5x Chief Information Security Officer Chief Technology Officer

Allan Alford is CISO and CTO at TrustMAPP, securing the business and creating a cybersecurity performance management product to enable security leaders to measure, manage, and report their security programs.

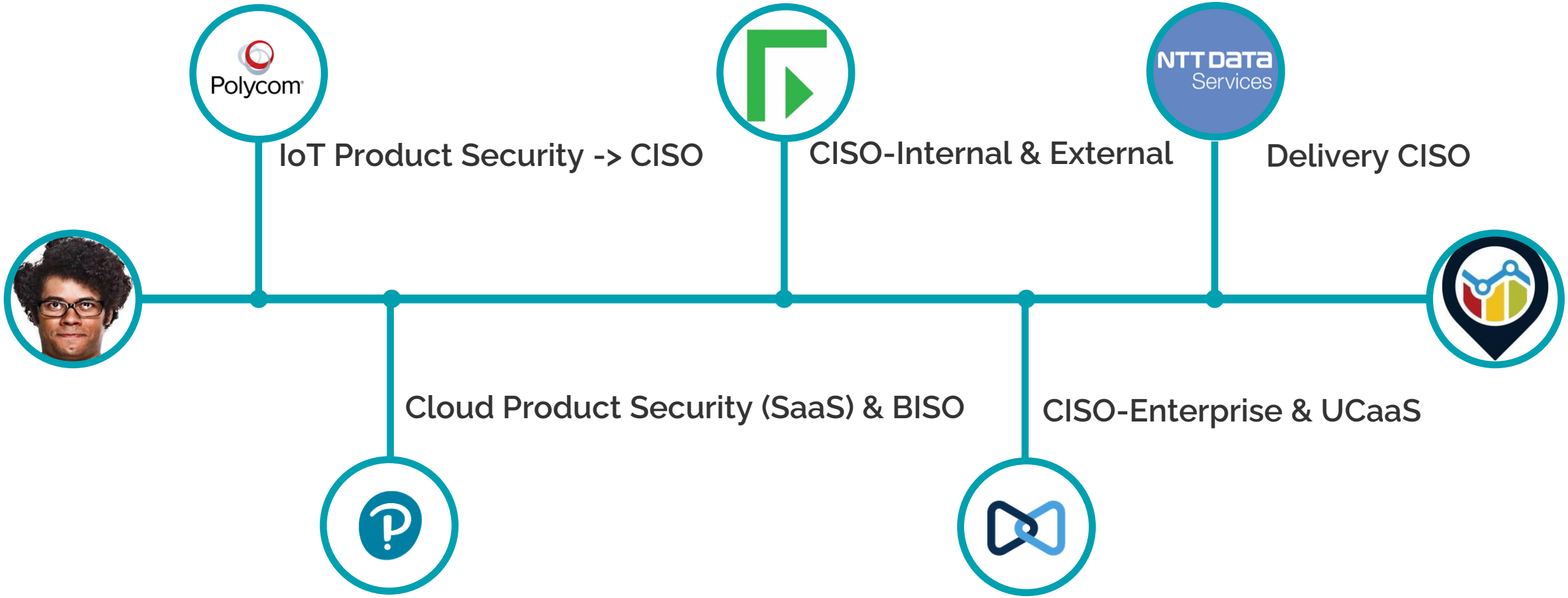
With 20+ years in IT and Engineering, Allan formerly served as Delivery CISO at NTT DATA Services, and CISO at Mitel, Forcepoint and Polycom. Allan has managed security strategy and led compliance with various frameworks and regulatory requirements such as NIST CSF, GDPR, ISO 27001, CIS, HIPAA, PCI, CMMC and others.

Allan also served at Pearson as Product Information Security Officer, where he created the security practice for a company-wide cloud transformation program. Allan also built and led the product security program at Polycom, integrating it fully into the product delivery process.

Allan holds a master's degree in Information Systems & Security, a bachelor's degree in Liberal Arts with a focus on Leadership.

Allan also serves on the advisory board for three different security vendors.

My Journey to CISO/CTO @ TrustMAPP
Creating Cybersecurity Performance Management



Hard-Learned Lessons

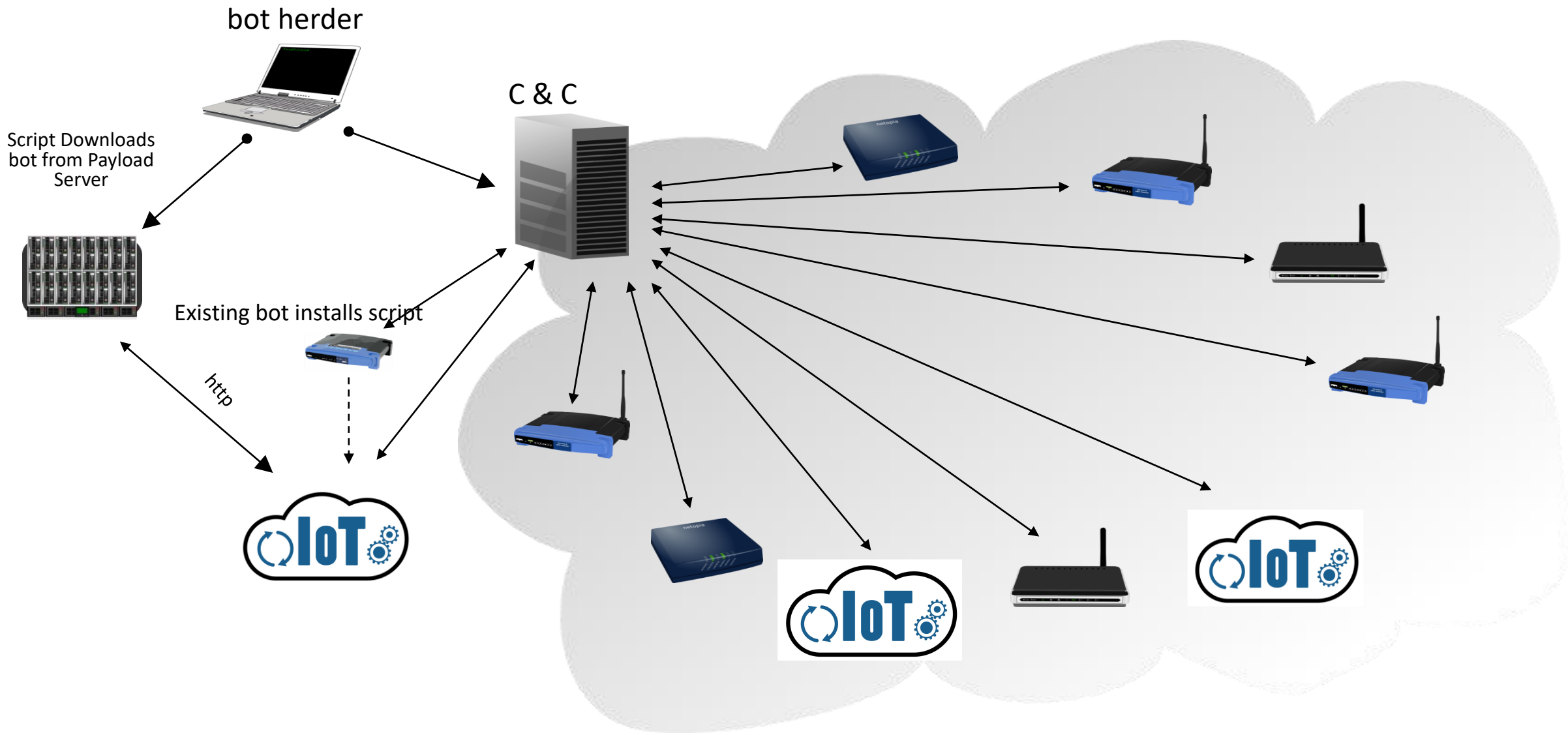
- The responsibility and burden of being in someone else's supply chain
- The importance of securing Internet of Things devices (IoT)
- The challenges all security practitioners face – the daily grind
- Zero-Day and/or Third-Party vulnerabilities

- Cyber hygiene ("The Basics")
- Compliance with frameworks
- Readiness and Controlled Reaction to Incidents

What I Learned – Third-Party Zero Day: Heartbleed

- Serious security bug in common encryption software routine
- Attackers can use this to extract passwords and encryption keys
- People used this to hijack VPN sessions
- Exploit code was circulating on the Internet
- It was no longer enough for a user to look for the lock icon in their browser – encryption was compromised!

What I Learned - IoT Compromise



What I Learned - Ransomware

- Globally, there were 304.7 million ransomware attacks in the first half of 2021, a 151% increase since 2020. (SonicWall)
- Ransomware attacks experienced annually by organizations have been on the rise since 2018, peaking at 68.5% in 2021. (Statista)
- 80% of organizations were hit by a ransomware attack in 2021. (Forbes)
- There were 121 reported ransomware incidents reported in the first half of 2021, a 64% increase from 2020. (PurpleSec)
- The FBI's Internet Crime Complaint Center (IC3) received 2,084 ransomware complaints in the first half of 2021. (FBI and CISA)

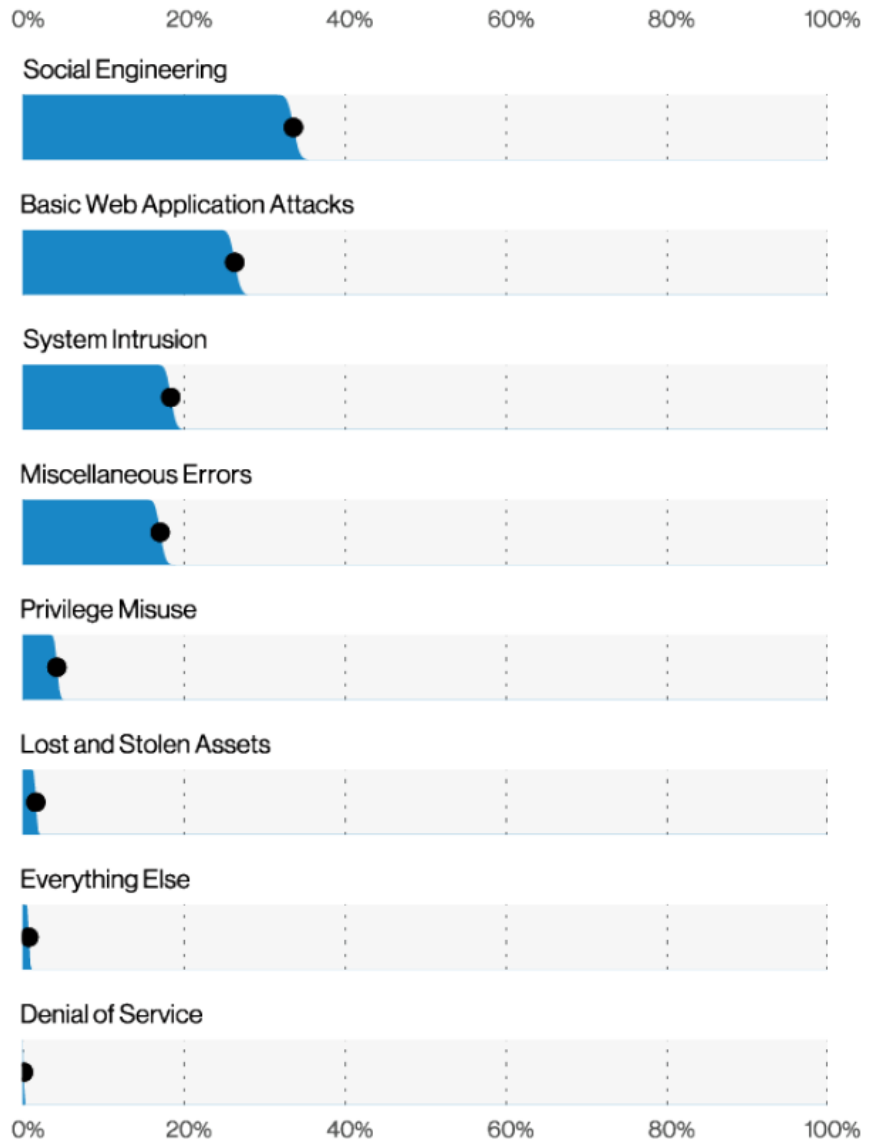
Ransomware Costs

- The total cost of a ransomware breach was an average of $4.62 million in 2021, not including a ransom. (IBM)
- The average cost for education institutions to rectify the impacts of a ransomware attack, including the ransom itself, was $2.73 million in 2021 — 48% higher than the global average for all sectors. (EdScoop)
- The 2,084 ransomware complaints received by the IC3 in the first half of 2021 amounted to over $16.8 million in losses. (FBI and CISA)
- Reported monetary losses to ransomware attacks increased 20% in the first half of 2021 compared to 2020. (FBI and CISA)
- Ransomware breach response costs took up 52% of the overall cost of a ransomware attack in 2020. (Corvus Insurance)
- Globally, no less than $18 billion was paid in ransoms in 2020. (EmiSoft)

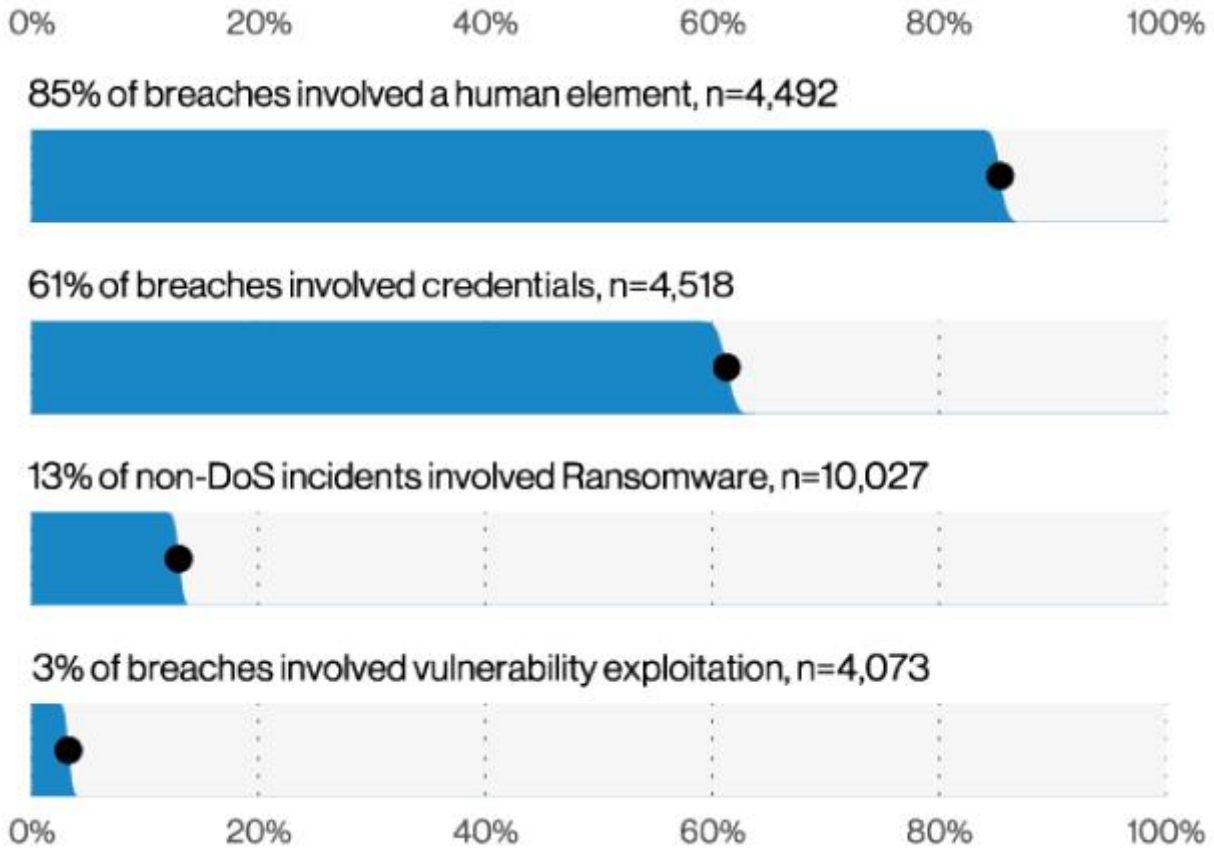
More Hard Lessons About Zero-Day (and Supply Chain Breaches)

- SolarWinds, a major US information technology firm, was the subject of a cyberattack that spread to its clients and went undetected for months, Reuters first reported in December. Foreign hackers, who some top US officials believe are from Russia, were able to use the hack to spy on private companies like the elite cybersecurity firm FireEye and the upper echelons of the US Government, including the Department of Homeland Security and Treasury Department.
- A vulnerability has been identified in Citrix Application Delivery Controller (ADC), formerly known as NetScaler ADC, as well as in Citrix Gateway, formerly known as NetScaler Gateway. This vulnerability, if exploited, could allow an unauthenticated party to perform arbitrary code execution. Please see this Citrix Knowledge Center article for reference and any questions.
- Much of the Internet, from Amazon's cloud to connected TVs, is riddled with the log4j vulnerability, and has been for years, Washington Post.

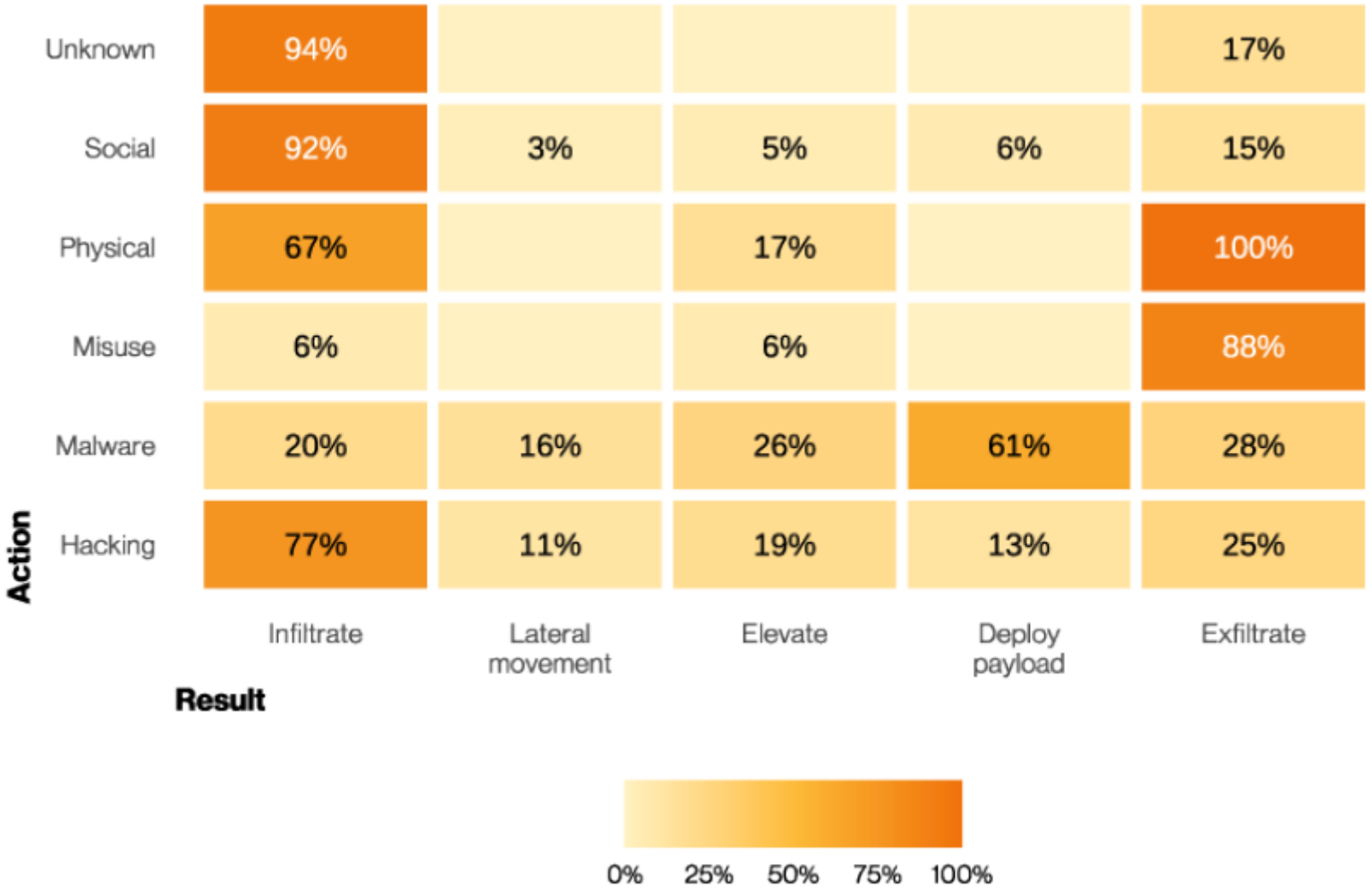
The Causes (From Verizon DBIR 2021)



More Breach Facts (DBIR 2021)



More Breach Facts (DBIR 2021)

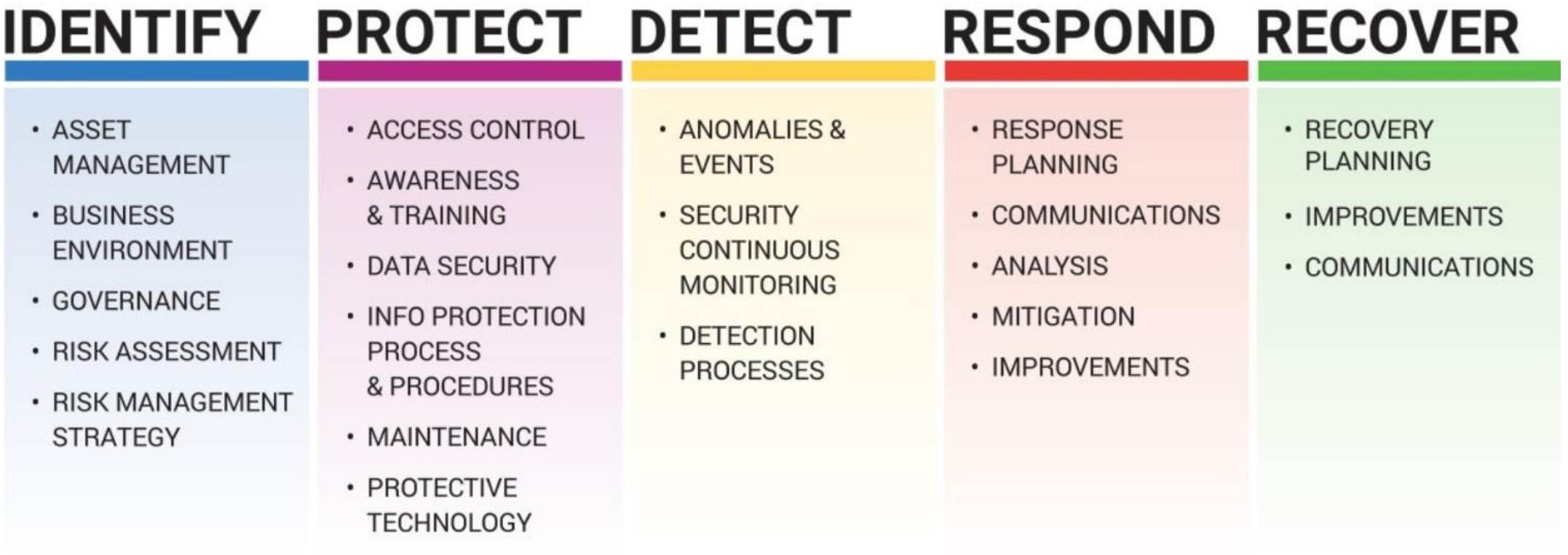


DBIR Conclusion:

The next time we are up against a paradigm-shifting breach that challenges the norm of what is most likely to happen, don't listen to the ornithologists on the blue bird website chirping loudly that "We cannot patch manage or access control our way out of this threat," because in fact "doing the basics" will help against the vast majority of the problem space that is most likely to affect your organization.

What Are “The Basics”?

NIST Cybersecurity Framework (CSF) v1.1



CIS Controls v8

A Simplified View

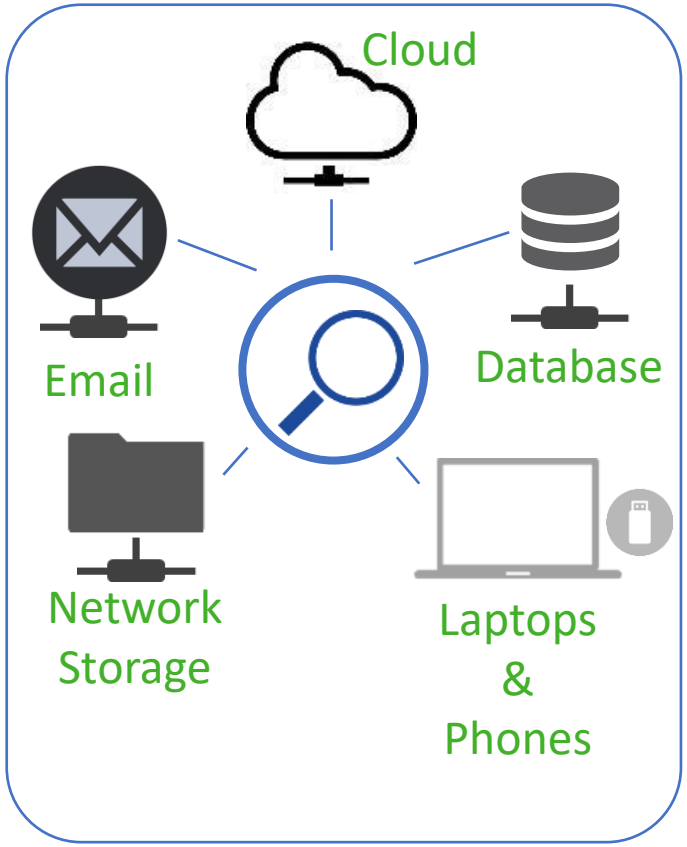
Hardware Asset Inventory – It's Boring, But It's Vital!

There is a reason both CIS and CSF start with Asset Inventory: You cannot secure what you don't know you have.

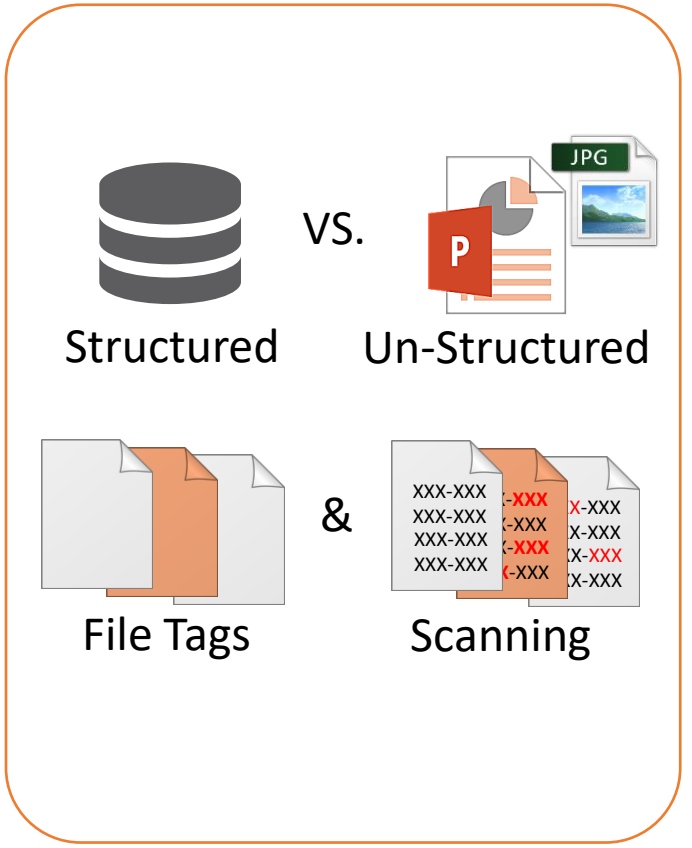
Asset inventory is the most important step in cybersecurity.

Start with what you know now, then grow!

Software Asset & Data Asset Inventory – It's A Bit Trickier – But Tools Are Available

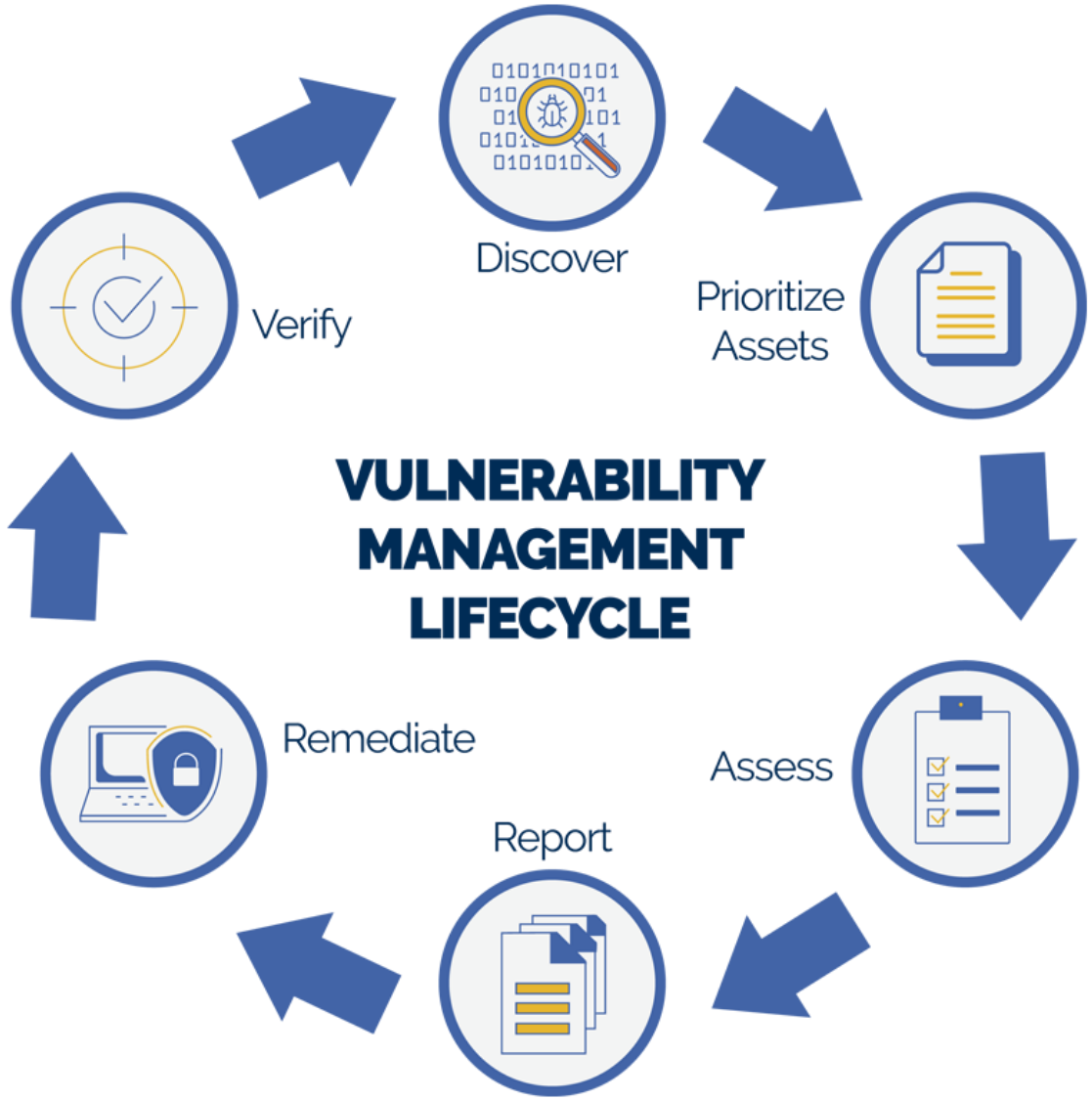


DATA IS EVERYWHERE, MANAGED BY MANY SOFTWARES



DATA IS NOT ALWAYS EASY TO FIND, SO LEVERAGE GOOD TOOLS

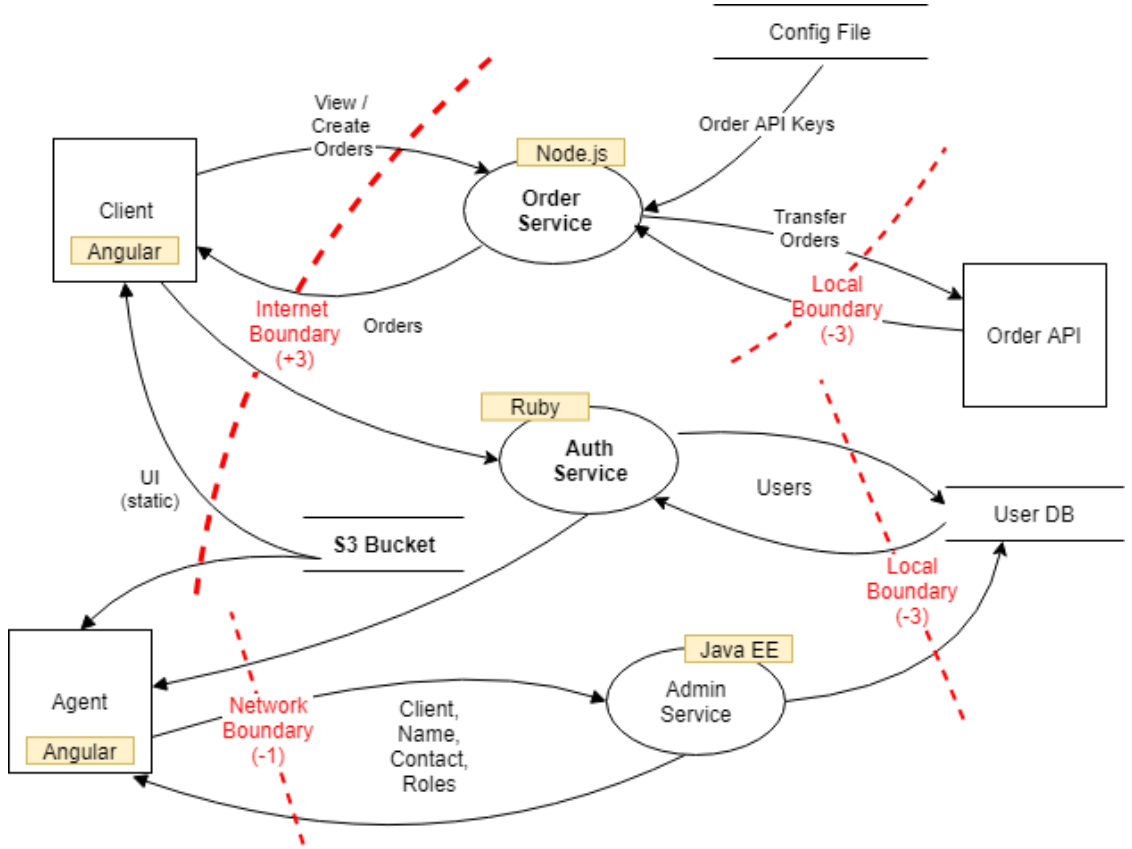
Vulnerability Management



Assess: Threat Modeling, BAS, Purple Teaming

As important as asset management and vulnerability management are, a threat modeling approach is equally valuable.

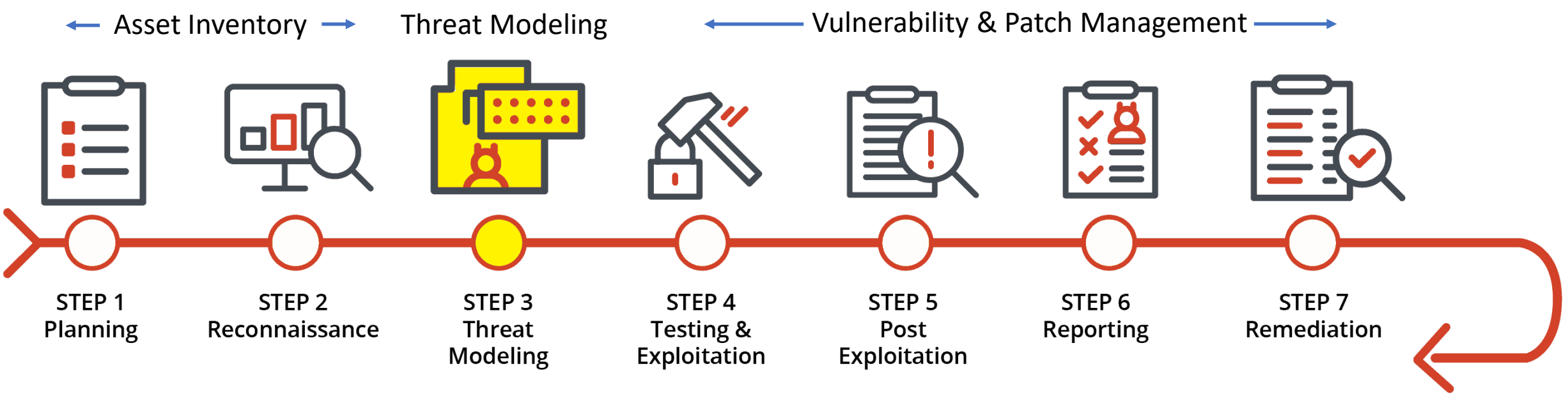
If you know your attack surface, and know the threats you face, you can begin to take steps towards securing your organization.



Vulnerability Management (and Patch Management)

This trifecta of asset inventory, threat modeling, and vulnerability (and patch) management feeds risk management and serves a key foundation in your security program.

Start with the systems most obviously related to your organization's central mission!



An Even More Simplified View…

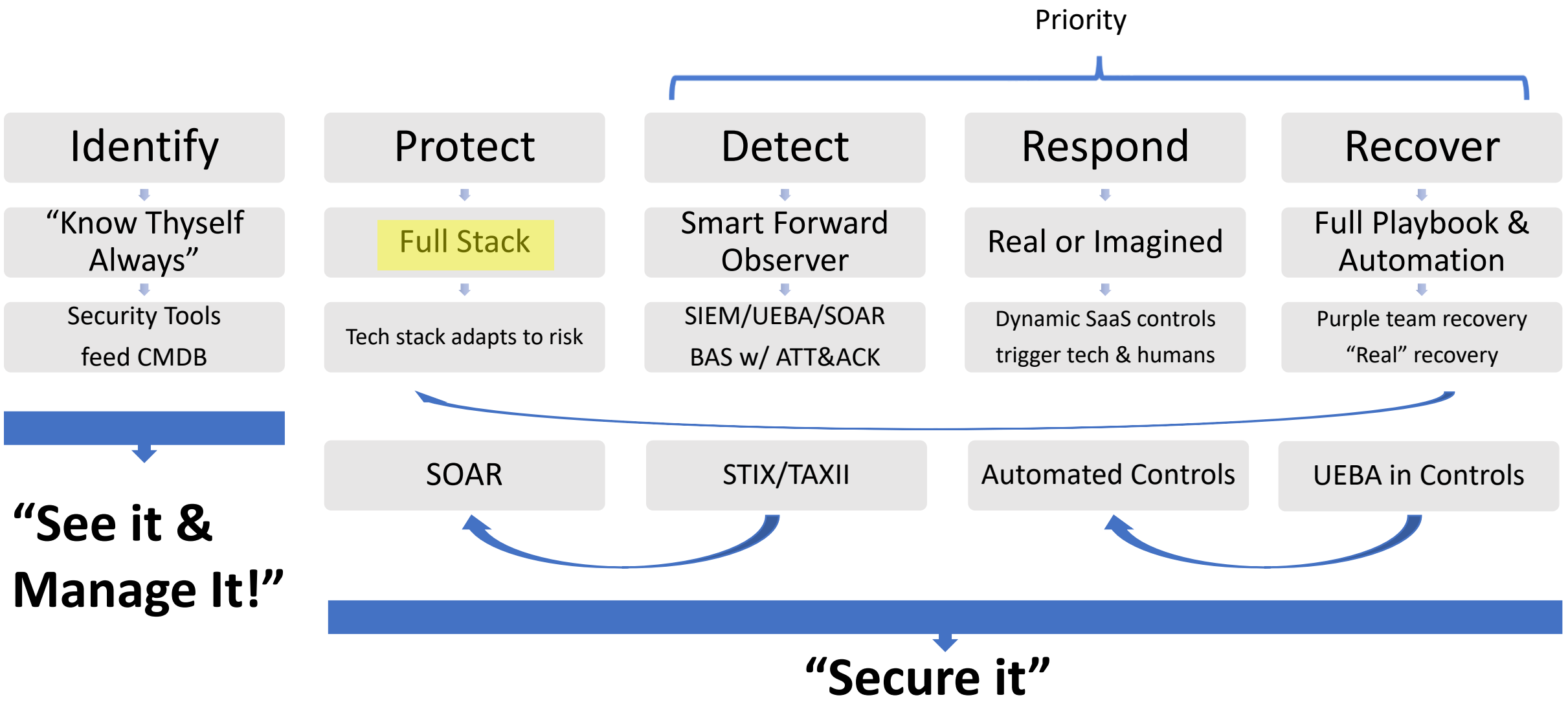
Better yet, a real-world model:

You have to **“See it”** ➡ Before you can **“Manage it”** ➡ And then you can **“Secure it”**

Common sense, right?

* Flagrantly stolen from Steve Williams over at NTT

The Non-Simple Version



“Full Stack” Simplified – “Minimum Viable Security” (“MVS”)

- Identity & Access Management at the heart of it all
- Secure Endpoint Management & Endpoint Protection
- SASE/CASB/(DLP)
- Email Hygiene & Security
- MFA/SSO/Passwordless

And Don’t Forget…

TECHNOLOGIES CHANGE

But People are the constant – so LEVERAGE them rather than BLAMING them!

People Aren’t the Problem - They’re the Solution

People are the best possible alternative to a tech stack.

Incentivize your employees while investing in them!

Training and enlisting champions is a great benefit both to the employee and to your organization.

Security Awareness Training

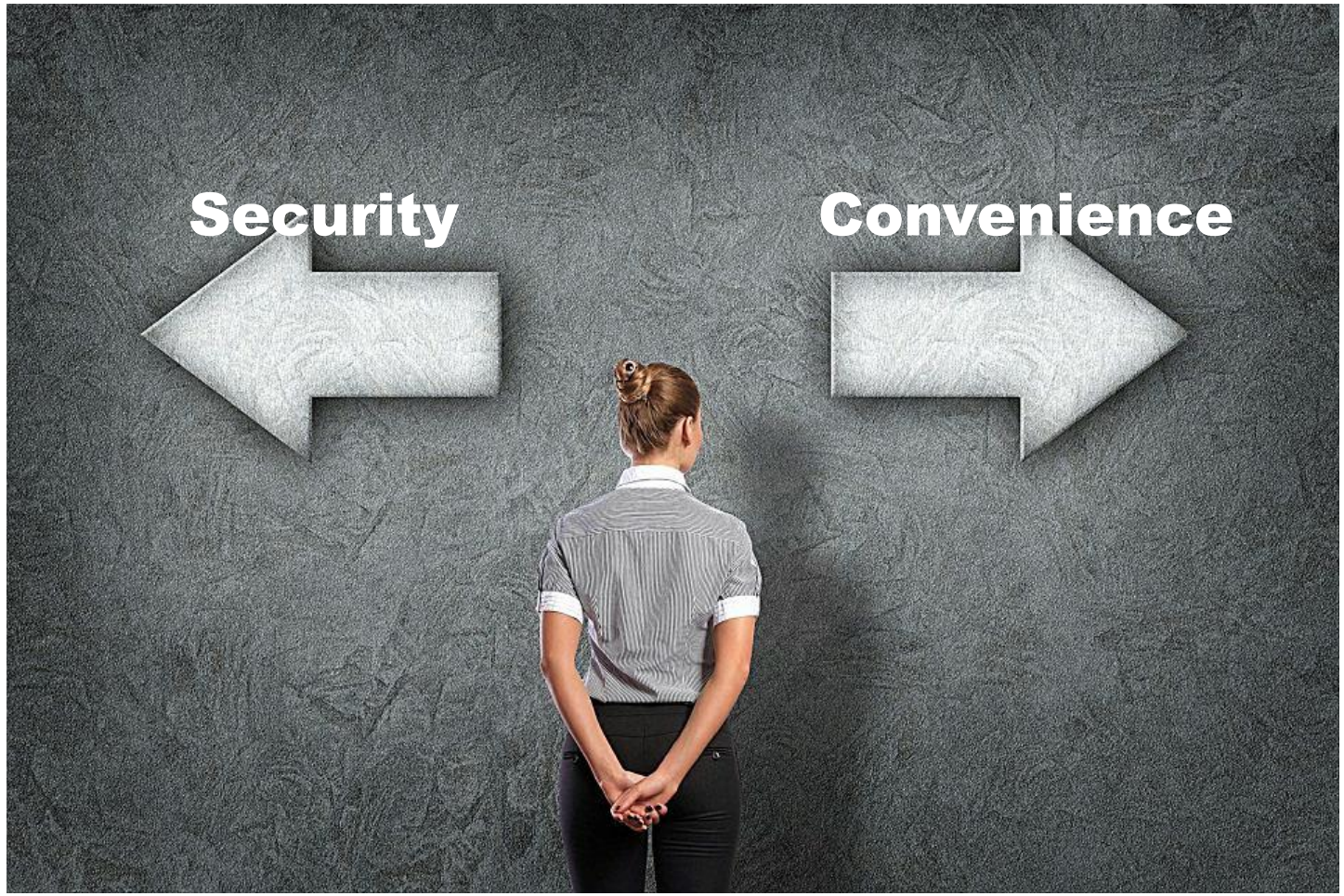
- Keep it SHORT and FUN and FREQUENT!
- Make it relatable with personal perspectives.
- Don’t deploy it in a punitive way.
- Have a small quiz after each microlearning.

Anti-Phishing Training

- WARN THEM AHEAD OF TIME
- Don’t Punish, Don’t Focus on Negative Results (Clicks)
- DO Focus on Positive Results (Reporting Rates)

- Do everything in your power to get the rest of the organization to not send emails that violate good practice, or to at least warn folks it’s coming.

ABOUT THAT PEOPLE FACTOR...



When given the choice of convenience or security, people will choose convenience.

MAKE SECURITY CONVENIENT. KEEP IT SIMPLE!!!

Ransomware & Zero-Day Solutions

- In Summary: CSF or CIS
  - Asset Inventory
  - Know and manage your attack surface
  - Stay as currently patched as possible and have mechanisms and processes in place to receive vendor patches and deploy them quickly

- But What else?
  - EXCELLENT monitoring
  - Solid Incident Response

Monitoring: Automation + People (UEBA + SOC)

SIEM vs. UEBA

UEBA is an integrated part of the Modern SIEM
to improve detection and response capabilities

SIEM

- Rule-based threat detection
- Used for a wealth of use cases within cybersecurity, compliance, IT operations and business analytics
- Can be tailored to meet specific analytics across all data
- Requires continuous tuning to ensure relevant analytics

UEBA

- Self-leaning threat detection
- Uses unsupervised machine learning
- Automatically assigns risk scores to entities and users
- Great at detection insider threats
- Doesn't require tuning to ensure relevant analytics

Incident Response Process

SIEM, UEBA, Threat Intelligence, BAS, Purple Teaming…

DETECT

RESPOND

RECOVER

Tier 1

Report Security Events which might become Security Incidents

Determine Incidents from Events

Tier 2

Report Security Incident to CISO

Improve capabilities of Detection and Response

Tier 3

Root Cause Analysis

Recovery

ALERT FOCAL POINT
Computer Security Incident Response Team

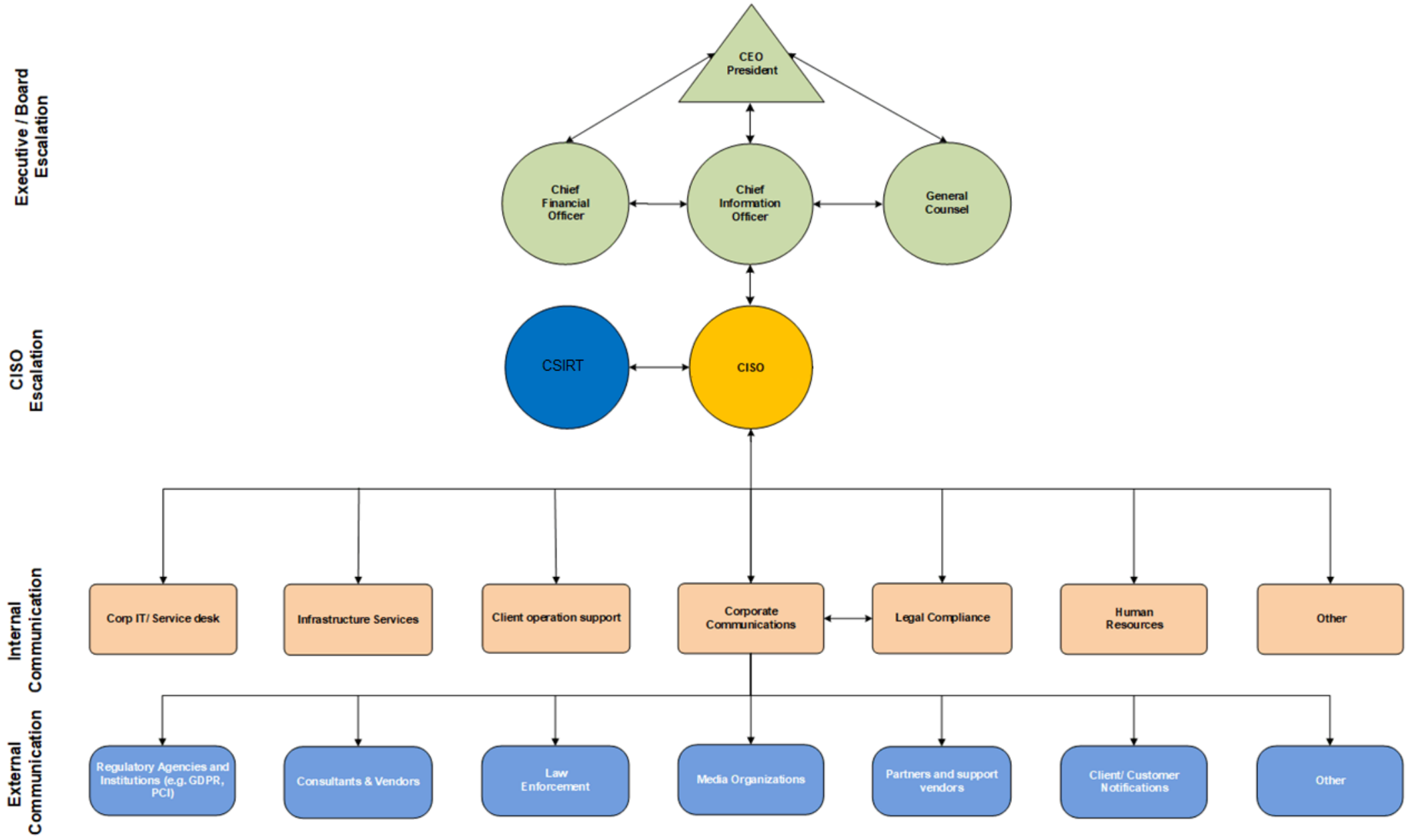
First Responder-Response Team
(Immediate Disposition Decision)
Incident (Low/Medium) or (High/Critical)?
Critical = Immediate broader alert
Others = Initiate deeper investigation

Threat Management Team
(Alert, Status, Risks, Impact)

Client Or Crisis Response Team
(Legal, Communication, IR, Exec)

Operations
Support CSIRT as needed

Incident Communication



Zero day solutions

- **1. AS TOLD BY SOLARWINDS: IT'S JUST AS CRITICAL TO BE DILIGENT WITH YOUR THIRD PARTIES AS YOU ARE WITH YOUR OWN ORGANIZATION. START BY IDENTIFYING GRAY RHINOS IN YOUR SUPPLY CHAIN ECOSYSTEM.**
- **2. AS TOLD BY AMERICAN BANK SYSTEMS (ABS): PATCH, PATCH, PATCH!**
- **3. AS TOLD BY COGNIZANT: TAKE BUSINESS CONTINUITY AND CRISIS MANAGEMENT SERIOUSLY, AS IT'S KEY TO PROVIDING SERVICES IN TIMES OF CRISIS.**
- **4. AS TOLD BY VIEWMEDIA: KNOW WHERE YOUR DATA RESIDES THROUGHOUT YOUR ENTIRE ECOSYSTEM.**

Ransomware solutions – from CPO magazine

Social engineering

When possible, find ways to give employees a glimpse into the mindset of an attacker. By role playing an attacker for a while, your employees will naturally become more skeptical of every interaction.

Unpatched software

Patch your internet-accessible software, operating systems, applications, browsers, browser add-ins, etc., as soon as a patch is available. Frequently scan your network for known, unpatched vulnerabilities that you may have missed. It can be mind-boggling to track all the software you're using and the many versions available. Use patch management software to streamline and automate patches.

Password guessing

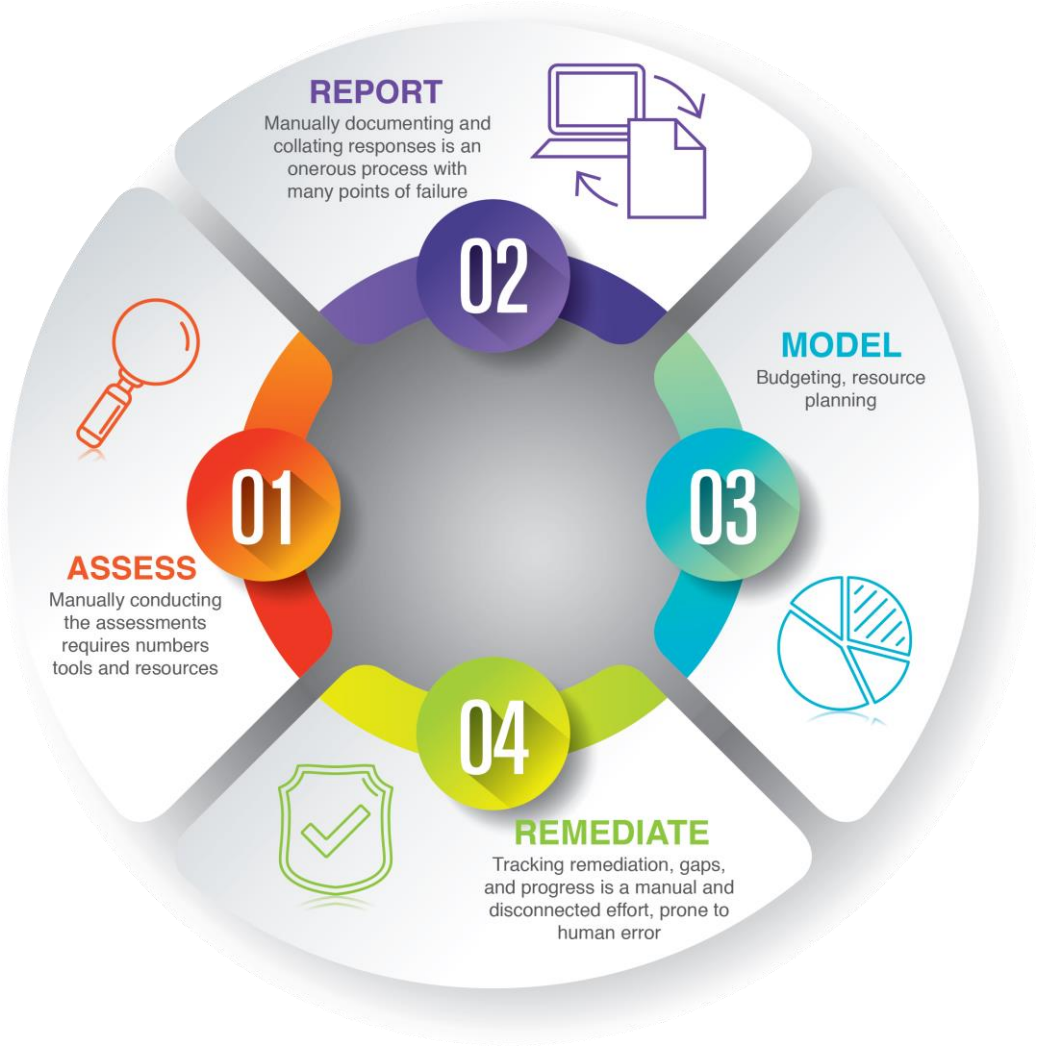
Educate employees about password best practices during your scheduled awareness training workshops.

Implement multi-factor authentication (MFA) where possible.

Implement account lockouts.

This Is A Lot To Manage…

Cybersecurity Performance Management



Cyber Security Performance Management

RISK ANALYSIS

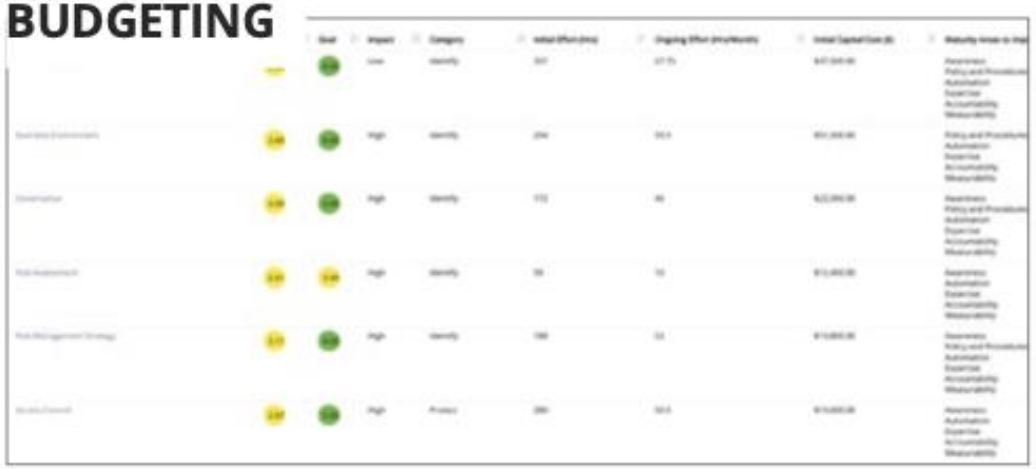
TRACKING COMPLIANCE & POSTURE IMPROVEMENT

RESOURCE PLANNING

WORKFLOW MANANGEMENT

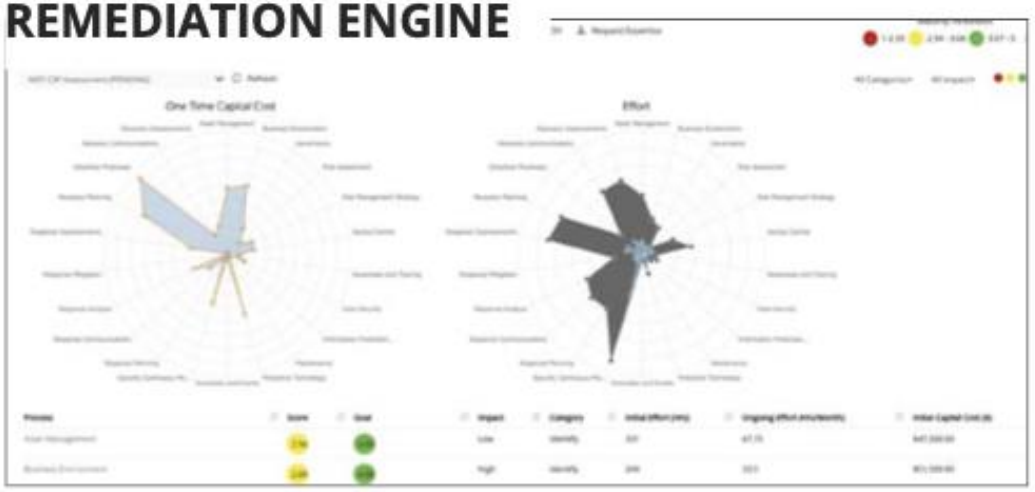
Cyber Security Performance Management

BUDGETING

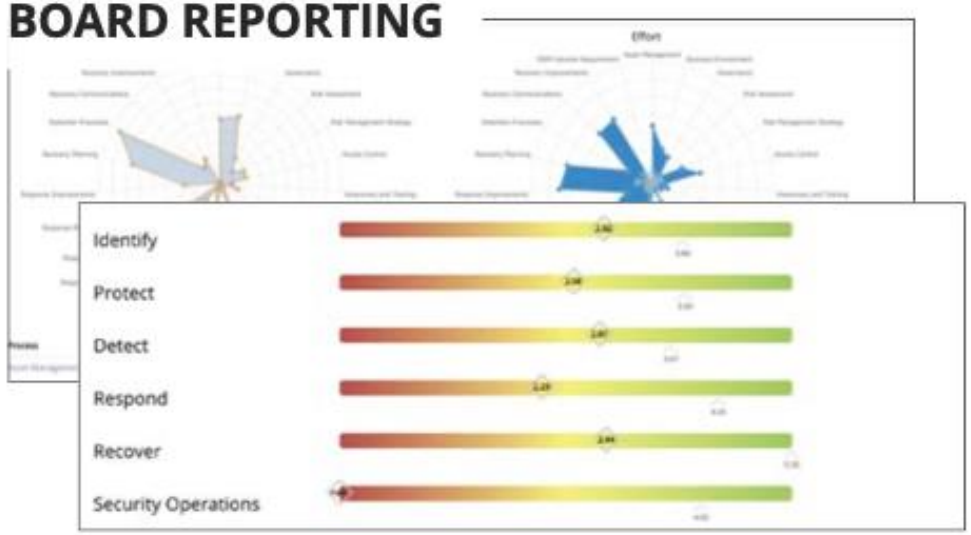


PROGRESS REPORTING

REMEDIATION ENGINE



BOARD REPORTING



Pre-Populated Recommendations

Response Analysis (RS.AN)	1.50	4.00	High	Respond	254.2	48.8

	RS.AN-1 Detection system investigation (v1.0 Maturity)	RS.AN-2 Incident impact (v1.0 Maturity)	RS.AN-3 Forensics performed (v1.0 Maturity)	RS.AN-4 Incident categorization (v1.0 Maturity)
	New Task	New Task	New Task	New Task
Maturity	2.00	1.00	1.00	2.00
Goal	4.00	4.00	4.00	4.00
Initial Effort (Hrs)	183	24.3	24.3	22.6
Ongoing Effort (Hrs/Mo)	40	3.2	3.2	2.4
Initial Capital Cost ($)	$76200	$2100	$2100	$1600
	(2->3) Further refine your own best practices within the policy and procedures (including investigating detection notifications) for the intrusion detection and prevention process (use guidance from NIST 800-94, if needed). Document your activities such as alerting and filtering on event data and reporting and prioritizing response to events. Find and use industry standard tools and automation for the intrusion detection and prevention process (including investigating detection notifications). Tools should cover automation of key areas such as logging of events, alerting and filtering on event data and reporting and prioritizing response to events. Document all skills needed for intrusion detection and prevention and arrange for and provide a plan for staff time and budget to train for this process (including investigating detection notifications). **(3->4)** Define internal best practices and continue to regularly update this well-defined, repeatable intrusion detection and prevention process (including investigating detection notifications). Seek to integrate with other tools (such as SIEM or ticketing system) and make sure existing tools and processes are used as planned. Cover the most critical areas of the intrusion detection and prevention process, such as logging, filtering of events and investigating detection notifications. Annually update skills requirements for intrusion detection and prevention to ensure process coverage remains up-to-date (including investigating detection notifications). Maintain training according to plans and encourage staff to share knowledge and seek certification (if available).	**(1->2)** Focus less on automation and more on identifying the key manual processes involved in incident response including incident impact evaluation and understanding. Define required skill sets for an incident response program (including incident impact evaluation and understanding). Provide annual training (ongoing management hours) to maintain these skills. **(2->3)** Use simple automation (such as spreadsheets) to manage responses (including reporting incident impact evaluation and understanding) to potential cybersecurity events. Research automation options (such as incident response management software) to manage security incidents. More fully define required skill sets (including reporting incident impact evaluation and understanding) for managing an incident response program. Boost annual training (ongoing management hours) to maintain these skills. **(3->4)** Use automation (such as incident response management software) to manage the response (including incident impact evaluation and understanding) to potential security incidents. Use data from other automated systems (such as security monitoring software) to aid incident response. Update annually the required skill sets (including incident impact evaluation and understanding) for managing an incident response program. Formalize standard annual training for all in this role (ongoing management hours) to maintain these skills.	**(1->2)** Focus less on automation and more on identifying the key manual processes involved in incident response including performance of incident forensics, to analyze the incident details. Define required skill sets for an incident response program (including performance of incident forensics, to analyze the incident details). Provide annual training (ongoing management hours) to maintain these skills. **(2->3)** Use simple automation (such as spreadsheets) to manage responses (including reporting performance of incident forensics, to analyze the incident details) to potential cybersecurity events. Research automation options (such as incident response management software) to manage security incidents. More fully define required skill sets (including reporting performance of incident forensics, to analyze the incident details) for managing an incident response program. Boost annual training (ongoing management hours) to maintain these skills. **(3->4)** Use automation (such as incident response management software) to manage the response (including performance of incident forensics, to analyze the incident details) to potential security incidents. Use data from other automated systems (such as security monitoring software) to aid incident response. Update annually the required skill sets (including performance of incident forensics, to analyze the incident details) for managing an incident response program. Formalize standard annual training for all in this role (ongoing management hours) to	**(2->3)** Use simple automation (such as spreadsheets) to manage responses (including reporting categorizing the incident as described in the response plan) to potential cybersecurity events. Research automation options (such as incident response management software) to manage security incidents. More fully define required skill sets (including reporting categorizing the incident as described in the response plan) for managing an incident response program. Boost annual training (ongoing management hours) to maintain these skills. **(3->4)** Use automation (such as incident response management software) to manage the response (including categorizing the incident as described in the response plan) to potential security incidents. Use data from other automated systems (such as security monitoring software) to aid incident response. Update annually the required skill sets (including categorizing the incident as described in the response plan) for managing an incident response program. Formalize standard annual training for all in this role (ongoing management hours) to maintain these skills.

Thank You!