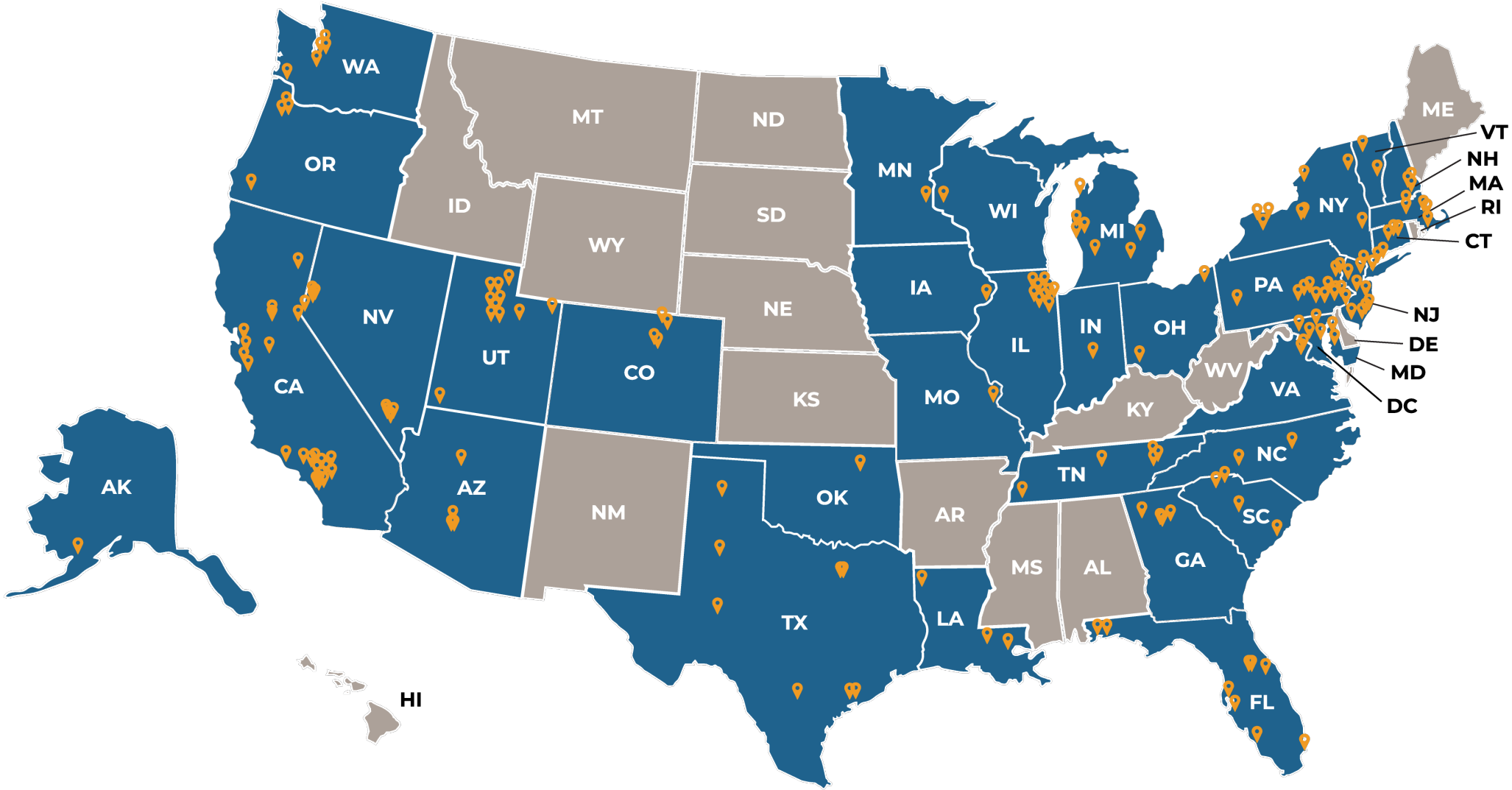
ALERAGROUP

Cyber Armor for your Business: How to Shield your Business as Cyber Attacks Rise

October 17, 2023

Welcome to clients & friends of our Alera Mid-Atlantic Region Partner Firms!



Have Questions?

During the webinar, feel free to:

- Enter your questions into the “Chat” feature in the Zoom Meeting
- All questions will be addressed during the last 15 minutes of our session

Reminders

Complete our 2-minute post webinar **SURVEY**. All completed surveys will be entered to win a **$100 Goldbelly Gift Card!**

Webinars

The 3 E's of Open Enrollment: Engage, Educate and Empower

October 19th, 2 PM – 3 PM EST

Culture, Communications and Technology: 3 Ways to Tie Benefits to Retention

November 16th, 2 PM – 3 PM EST

Quarterly Compliance Update

December 5th, 2 PM – 3 PM EST

A Look Ahead to 2024: What's on the Horizon in Employee Benefits

December 21st, 2 PM – 3 PM EST

Upcoming Events

Alera Group's 2023 Property and Casualty Market Outlook Report

What you'll find in this report:

- Updated pricing and capacity conditions in the P&C Insurance market
- Valuable insights into what's happening in the market
- Key factors driving these conditions
- Strategies your organization can act on

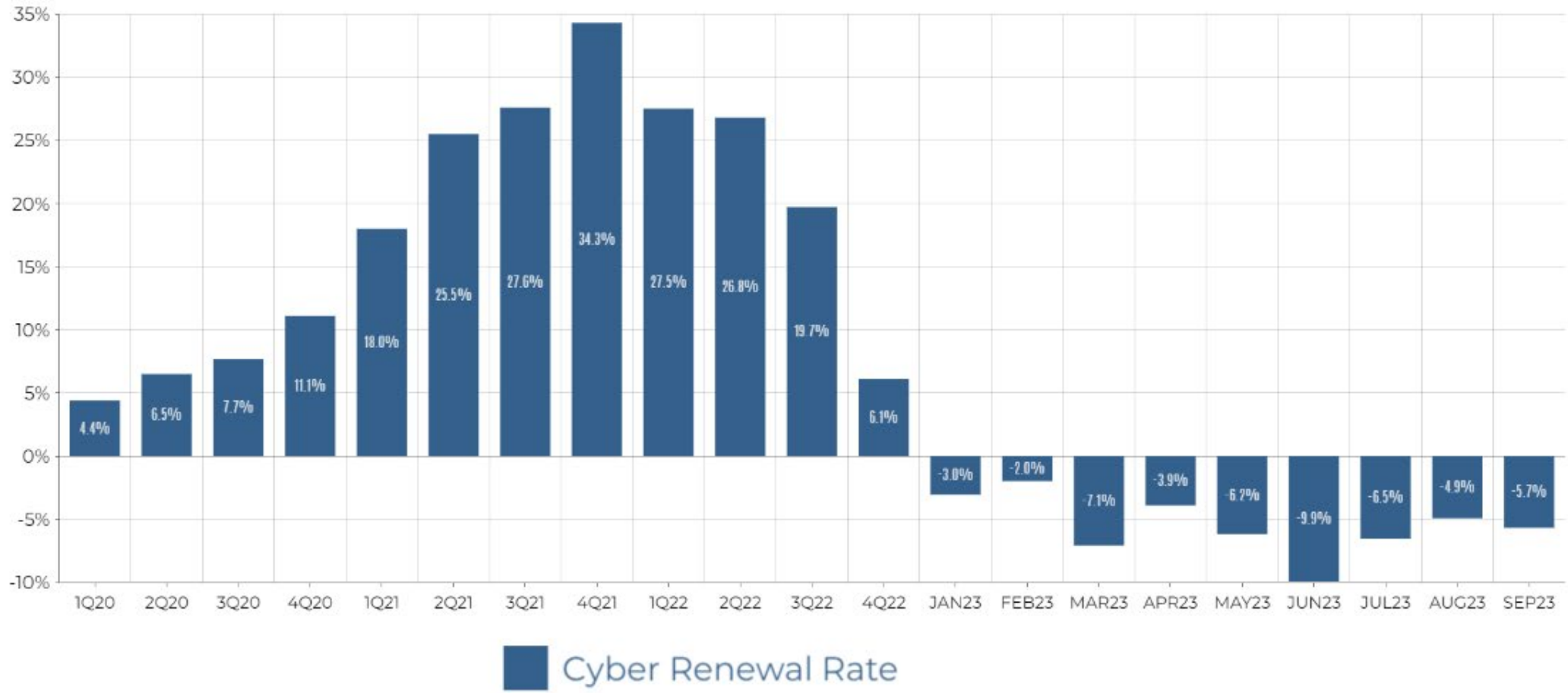
Please contact your Alera Account Representative for more information

Welcome

Gene Nosovitch, *Alera Group*
Brian Block, *Alera Group*
Matt Grist, ACA Aponix

Cyber Insurance Renewal Rates

Rate increases decelerated through 2022 and turned negative in 2023



Cyber Risks Back on the Rise

Clorox Warns of Accruing Costs From Cyberattack

Hack came amid a $500 million digital overhaul at the consumer products maker

MGM Resorts Refused to Pay Ransom in Cyberattack on Casinos

Fallout will have a $100 million negative impact on quarterly earnings, Las Vegas-based company says

Hackers With AI Are Harder to Stop, Microsoft Says

New cybersecurity research shows artificial intelligence and new encryption tactics test corporate defenses

- Hackers are using large language models similar to those in generative AI tools to speed up elements of cyber attacks like writing phishing emails or creating malware, making it easier to carry out hacks
- General data exfiltration attacks, where hackers steal data and demand ransom payments from victims, doubled between November 2022 and June 2023

Coalition Reports SMB Ransom Demands Up 50%+ in 1H23

AVERAGE RANSOM DEMAND 1H 2023

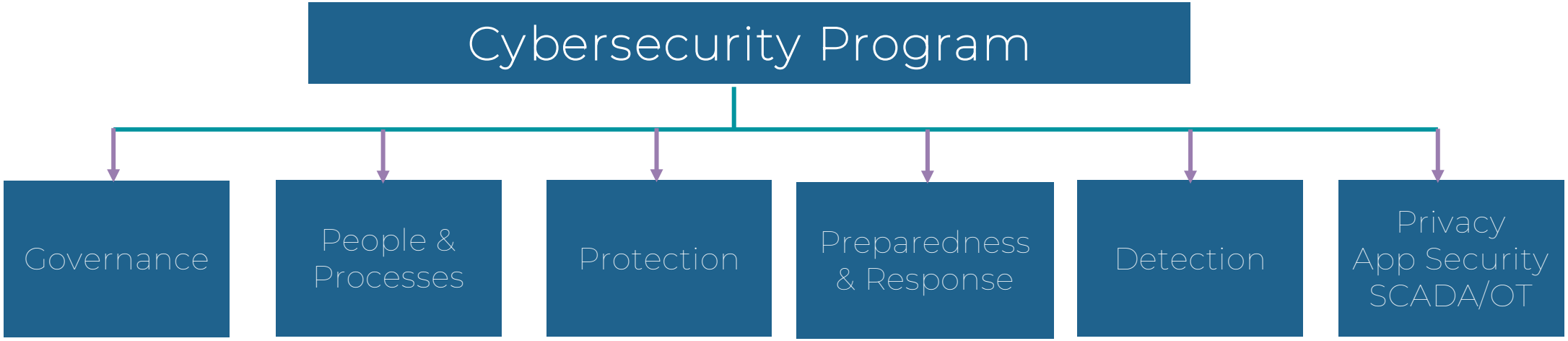
ACA Aponix®

Cybersecurity & Risk

ACA Aponix® provides cybersecurity risk programs, data privacy compliance services, vendor and M&A diligence services, portfolio company oversight, network testing, and advisory services for companies of all sizes. Our award-winning solutions are designed to help firms uncover risks and identify deficiencies in their cybersecurity policies, procedures, and controls.

ALERAGROUP

Building a Robust Cyber Program



Governance

Policies and procedures to make sure cyber risks are identified and appropriately addressed, including assigning responsibilities, risk assessment, KPIs, and management of third parties

What to consider

- Program Ownership
- Policies
- Program Management
- Cyber Risk Management
- Asset Management
- Third-party Risk Management (TPRM)

What we see

- Cybersecurity is still considered an IT problem (becoming rarer).
- Most have policies, fewer actively track cyber risks in business terms.
- Asset management is challenging at scale and requires some level of automation.
- Third party risk management is often an areas of weakness.
- Policies are not effectively communicated.

What we recommend

- Make cybersecurity an executive/board owned item.
- Translate cyber gaps and issues into business risk.
- Establish a TPRM policy, working with legal and procurement functions.
- Ensure cybersecurity policy requirements are understood and acknowledged by all employees – either via training, compliance tracking and/or an employee handbook.

Focus area – Third Party/Supply Chain Risk

- Establish a TPRM program which includes cyber due diligence.
- Create a list of suppliers and service providers.
- Identify responsible staff for managing third-party life cycle:
    - Third-party selection and contracting
    - Due diligence
    - Ongoing performance monitoring and diligence
- Take a risk-based approach – understand the inherent risk of each third party and tier for prioritization.
- Set a re-review cadence for top tier vendors – not just an activity at the point of procurement.
- Set minimum cybersecurity requirements.
- Ensure contracts hold third parties accountable.
- Request SOC reports and other outside audit reports but don't limit due diligence to review of those materials.

People & Processes

Policies and procedures around mitigating risks posed by employee error or fraud

What to consider

- Training & Awareness
- User Behavior Testing & Analysis
- Onboarding and Offboarding Processes
- Business Process Controls

What we see

- Most organizations understand the importance of training, but it can still be seen as a one-off 'tick the box' activity.
- Phishing tests are common and becoming the norm.
- Onboarding and offboarding processes are usually defined, but execution is manual and prone to error.
- Business process controls are often reliant upon the knowledge and behaviors of key individuals, rather than defined processes.

What we recommend

- Train employees regularly – little and often as well as formal annual events.
- Try to instill a cyber security culture within the organization.
- Conduct different types of phishing tests and include other social engineering where possible.
- Define and document simple payment control processes, encourage adherence, and support them with technical controls where possible.
- Consider impacts of working from home on employee behavior and process controls.

Focus area – Business processes and training

Mitigating Business Email Compromise

- Use strong password practices.
- Enable MFA and disable legacy authentication.
- Conduct employee training.
- Implement email authentication methods to minimize risk of spoofing.

Safeguarding Against Payment Fraud

- Minimize # of employees authorized to process and approve transfers and payments.
- Set simple checklists to follow and never allow exceptions – culture.
- Establish bank withdrawal limits.
- Require dual authentication of all payment requests.

Training

- Make it interesting!
- Consider ongoing micro-training.
- Make it relevant – both to the context of your business and to employees' daily lives.
- Use real examples to bring the risk to life.
- Track and record completion of training as a KPI.
- Conduct specialist training for high-risk/high-privilege roles.
- Enable what you train – i.e., support training with tools and processes.

Protection

Technical controls to safeguard data and systems such as encryption, access control, firewalls, and antivirus

What to consider

- Technical Configuration Standards & Procedures
- Change Control Management
- Mobile Device Management
- Remote Access
- Data protection
- Email security

What we see

- Change control is often absent or informal.
- Mobile device and BYO policies are sometimes written, but enforcement can present issues with employees.
- Remote access is usually secured by MFA, but the increase in cloud services has reduced the need for VPNs.
- Encryption is generally in place by default.
- Emails are scanned and controlled, often via native tools (E.g., M365, Google Workspace).

What we recommend

- Underpin policy statements with baseline builds and procedures.
- Focus on email as a primary attack vector and look beyond default controls.
- Always mark external emails.
- Encrypt by default and link this to access controls.
- Track and manage changes to prevent security gaps and ‘exceptions’.

Protection (cont.)

Technical controls to safeguard data and systems such as encryption, access control, firewalls, and antivirus

What to consider

- Identity Access Management
- Privileged Access Management
- Authentication
- Endpoint Protection
- Network Security
- Patch Management
- Physical & Environmental Security

What we see

- Fewer organizations have a robust access review in place.
- Privileged access is not treated as different from standard access.
- MFA is increasingly common.
- Traditional network controls are changing as SAAS use increases – but controls over what employees can access varies.
- EDR use is increasing.
- Patching is improving.
- Physical security is not considered due to WFH.

What we recommend

- Set up access review policies and processes.
- Understand what privileged accounts you have.
- Set access and browsing controls to reduce risk – increasingly this needs to be on the endpoint.
- Configure EDR to isolate and contain first.
- Set patching as a KPI and include 3rd party software.

Focus areas – Authentication (MFA), endpoint protection and patching

Endpoint Detection & Response (EDR)

- An EDR solution is a baseline control and should be running on all endpoints.
- Configure EDR to contain and isolate by default. Malware moves at computer speed, your protection needs to as well.
- Never allow users the privilege of disabling EDR.
- Even where EDR is contained by default, outputs and alerts should be monitored and responded to.
- Link your EDR to a broader monitoring, alerting, and incident response plan.

MFA

- A 'red line' for insurers.
- Should be enabled wherever possible and certainly for any remote and/or privileged access.
- Be wary of authentication fatigue – use number matching.
- Train users on how attackers will attempt to defeat it – e.g., fake helpdesk asking for access codes.
- Consider physical tokens for certain roles and access.

Patching & vulnerability management

- Set formal policy requirements for the remediation of vulnerabilities.
- Measure remediation via KPIs.
- Ensure that all vulnerabilities are considered.
- Patch both OS and third-party software.
- Ensure that ownership and responsibility for vulnerability remediation includes system and business owners.
- Link to risk management.

Preparedness & Response

Planning, and testing plans, for disasters and incidents; backups and other measures to enable recovery to agreed timeframes; acquisition of cyber insurance if appropriate

What to consider

- Business Impact Analysis (BIA)
- Backups
- Business Continuity Planning (BCP)
- Incident Response (IR)
- Disaster Recovery (DR)
- Cyber Insurance

What we see

- Most organizations have something in place, but it is often informal.
- BC and DR are usually better understood than cyber incident response.
- Cyber incident response is too often seen as something for IT to handle.
- Incident response plans aren't practiced frequently enough.
- Backups are conducted, but recovery is not being tested.
- The need for external support is sometimes an afterthought.

What we recommend

- Base your response plans on a Business Impact Assessment (BIA).
- Document response plans and train employees on how to implement them.
- Protect backups as you would production systems.
- Test recovery from backups in line with the BIA.
- Practice incident response via regular exercises.
- Include third parties and your supply chain in all the above.

Focus areas – Backup and recovery

- Derive backup and recovery requirements from the BIA.
- Protect and secure backups as one of the most critical aspects of your inventory.
- Consider the 3, 2, 1 rule: 3 copies of data, 2 different media with 1 physically separate.
- Measure successful backups as a KPI.
- Test recovery from backups regularly.
- Include a complete rebuild of the impacted application, asset, etc. as part of recovery requirements.
- Ensure that recovery from backup follows a defined process, including who authorizes recovery.
- Include backups as part of an overall resiliency program.

Detection

Monitoring for potential threats and indicators of ongoing attacks; identification and remediation of vulnerabilities

What to consider

- Threat Intelligence & Management
- Vulnerability Management
- Logging
- Monitoring & Detection
- Penetration Testing

What we see

- Vulnerability management is still seen as an IT problem to solve.
- Logging requirements are often not defined.
- Monitoring can vary from 24/7 SOC to an IT team that will look at alerts when they have the time.
- Outsourcing of SOC is increasingly common.
- Penetration testing and red teaming can help identify gaps and bring the threats to life.

What we recommend

- Set KPIs, risk tolerance, and business ownership for the remediation of vulnerabilities.
- Ensure logging parameters align with the information to be captured.
- Make sure your monitoring meets your risk appetite and empower the SOC to act.
- Use pen testing to provide assurance around cyber programs and test your systems from an attacker's point of view.

Focus areas – Monitoring

- There is an increasing expectation that monitoring should augment security tools. This allows for alerts to be responded to in a timely manner, but also accounts for indicators of compromise (IOC) to be assessed.
- Be aware not all malicious activity will trigger a clear alert.
- Utilize analysts to triage alerts.
- Consider utilizing a Security Operations Center (SOC) that can provide 24/7 coverage as well as human expertise.
    - SOC as a service and/or a MSSP may be the right solution as in-house SOC can be challenging.
- Augment existing incident response plans with monitoring.
- Put in place some level of response to alerts.

Other domains to consider

Application and product security

- Ownership
- Policy and Process
- Developer Support for Secure Development
- Security by Design
- Production and Development Environment Controls
- Testing

SCADA and OT

- Ideally covered by all the domains above.
- Challenges with the need to maintain separation.
- A key attack target.
- Needs to be considered alongside corporate IT.
- Legacy systems present challenges.

Privacy

- Deserves a presentation of its own.
- Security enables some aspects of privacy (e.g., encryption, breach notification, etc.).
- Well established in Europe, but newer (and potentially more complex) in the US.
- Should be run as a program with supporting operational processes.
- Data governance is a key element.

Q&A: Thank You for Attending

Complete Your **Survey** – We Value Your Feedback!

Follow Us