Cybersecurity Threat Landscape & Risk Management

Steven J. Ursillo, Jr.,
Partner, National Leader of Information Assurance & Cybersecurity

Cherry Bekaert
Your Guide Forward

1

Meet the Speaker

Steven J. Ursillo, Jr.

Partner, National Leader of Information Assurance & Cybersecurity

Certifications: *CPA, CGMA, CITP, CIA, CFE, CISA, CISM, CISSP, CGEIT, CRISC, CEH, CCSFP*

Steve specializes in risk management, internal control over financial reporting, information system security, privacy, cyber fraud prevention and detection, security and privacy governance, and IT assurance services.

With more than 20 years of experience, Steve provides a variety of IT audit and security services for his clients across multiple industries. His background and knowledge with risk assurance and advisory engagements include information security readiness, cybersecurity, security and privacy attestation services, third-party assurance including ISO 27001/PCI/NIST/CMMC/HITRUST/HIPAA HITECH Security Assessments, cyber risk assessments, vendor risk assessments, disaster recover reviews, privacy reviews, Service Organizational Control (SOC) reporting including SOC 1, 2 & 3, ISAE 3000 & 3402 as well as other types of attestations and readiness assessments. In the area of information security, Steve's experience ranges from security consulting and implementation to security assessments involving network and attack and penetration testing.

2

2

Focus and Objectives

Today's Agenda

- What are we worried about for the new normal?
- Understanding the current threat landscape and remote workforce implications
- Mitigation techniques
- Cyber governance and why its important to your organization
- Questions

3

3

Polling Question #1

- ***I stay current on the latest cybersecurity risks and threats:***
  1. Always
  2. Most of the time
  3. Some of the time
  4. Rarely

4

4

4

So… What Are We Worried About (For the New Norm)?

- Maintaining service commitments (pandemic)
- What are the system boundaries and where are our people?
- Data management (where is our data?)
- Loss of private, confidential, customer data
- Third party dependencies (vendor and supply chain management)
- Spear phishing attacks
- Attack sophistication and evolution
- Data breach (lack of incident response)
- Strategy, compliance, operational, financial, reputational risk considerations
- Lawsuits and legal implications
- Proper risk mitigation
- Negative publicity
- Are we doing the right thing?

5

5

Common Cybersecurity Definitions, Background Landscape and Attack Vectors

Cherry Bekaert
Your Guide Forward

6

Cybersecurity Definitions and Background

Threat Actor: Malicious person or entity responsible for a cyber event or incident

Attack Vector: Method of achieving unauthorized network access

Attack Surface: The total number of attack vectors an attacker can use to manipulate a network, computer system, or extract data

Breach versus Incident: [1]

- **Incident** – event that compromises the integrity, confidentiality, or availability of an information asset
- **Breach** – an incident that results in the confirmed disclosure of data to unauthorized parties

Source [1]: https://insights.integrity360.com/incident-or-breach#:~:text=Incident%3A%20A%20security%20event%20that,data%20to%20an%20unauthorised%20party.

All other source: https://www.upguard.com/blog/attack-vector

7

7

How Do Attackers Exploit Attack Vectors?

Passive Exploits

- Attempt to gain access, but do **not** affect system resources
- Examples include:
  - phishing
  - social engineering
  - Typo-squatting (fake URL addresses)

Active Exploits

- Attempts to alter a system or affect its operation
- Examples include:
  - Malware
  - Attacking unpatched vulnerabilities
  - Ransomware

8

8

Cybersecurity Threat Landscape & Cybersecurity Recent Trends

Cherry Bekaert
Your Guide Forward

9

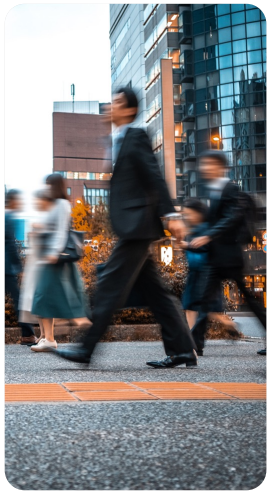
Trends

The variety, sophistication and maturity of attacks are bewildering

- Pandemic considerations (remote workforce, supply chain challenges. phishing and other scams)
- Data boundary challenges
- Regulatory attention
- Ransomware as a Service (RaaS)
- Proliferation of IoT and OT Devices
- Automated attacks
- Sophisticated financial attack techniques
- Malware for mining crypto currency
- Supply chain attacks
- Sensitive data in public cloud
- Cyber espionage on the rise
- Phishing attacks thrive across social media platforms
- Web apps evolving faster than web security

10

10



Todays Mobile Warrior

- Pandemic – a catalyst of change
- Organizations forced to accommodate at a rapid pace (remote access considerations)
- Supply chain challenges (systems and technology)
- Organizational culture
- Increased attack surface (IOT, home networks, personal devices, VPN, etc.)
- Attacks focusing on the user – end point and network

11

11

Who is Responsible?

Approx. 80% Outsiders

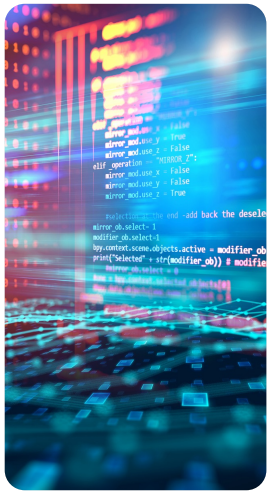
- Organized Crime/Terrorists *
- State Affiliated/Nation State
- Hacktivists/Activist
- Unaffiliated
  - Hackers/Crackers
  - Competitor (Espionage)

Approx. 20% Insiders

- Employee
- Disgruntled Employee
- Past Employee
- Vendor / Customer (Trusted 3rd Party)

12

12



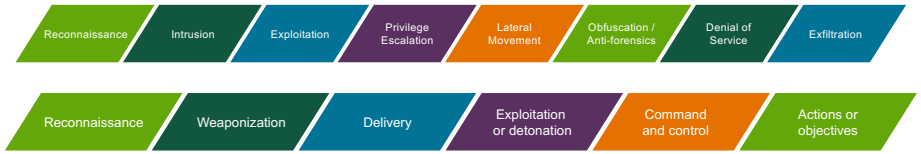
Adversary Objectives

- Monetization of data (PII, PHI high valued data)
- Theft and sale of assets
- Illicit transaction and financial fraud (Business email compromise)
- Disruption of operations
- Brand destruction

13

13

Attack Patterns and Kill Chain



14

14

Cybersecurity Costs and Concerns

83%	$4.35M	19%	83%	19%
of organizations studied have had more than one data breach	Avg cost of a data breach in 2022	of breaches occurred because of a compromise at a business partner	Percentage of organizations that have had more than one breach	Frequency of breaches caused by stolen or compromised credentials

Source:
IBM The Cost of a Data Breach, 2022

15

15

Trends for Exploitation

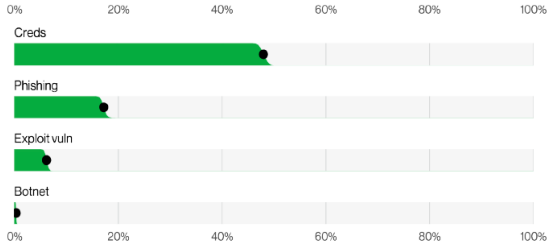


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

Source: 2022 Verizon Data Breach Report

16

16

Polling Question #2

- ***When it comes to a potential material cybersecurity incident, my organization:***
  1. Is well prepared, bring it on!!!
  2. Is fairly mature and has tested the plan on a few occasions
  3. Procedures are ad-hoc but can respond based on the circumstances
  4. Has not performed any preparation

17

17

Cybersecurity Threat Landscape Risks, Threats, Attack Vectors, Mitigation

Cherry Bekaert
Your Guide Forward

18

Common Attack Vectors

Top Risks

- Supply Chain Attacks
- Access and Authentication Management
- Outsourcing/supply chain
- Cloud apps/email/social media
- Poor patching processes
- Badly coded applications
- Consolidation and M&A
- Failing to Plan
- End users (awareness, disgruntled)

Top Threats-Summary

- Credential Attacks (User, PA, VPN, RA)
- Phishing/variants (Human factor)
- Distributed Denial of Service
- Network, system and web application Attacks
- Malware:
  - No footprint malware
  - Malware infiltration and persistent threats
- Targeted Ransomware
- Business email compromise
- ATO (Account Takeover Attacks)
- Shadow IT
- IOT and IoMT device hacking

19

19

Common Attack Vectors – (Continued)

Credential Attacks

Compromised Credentials

- Usernames and/or passwords exposed (in data leaks, phishing scams or by malware)
- Control through:
  - Password Manager
  - Multi-Factor Authentication

Weak Credentials

- Lack of adherence to industry best practices
- Control through:
  - Training and awareness
  - Group Policy or Configuration requirements
  - Password Manager
  - Privilege Access Management
  - Single-Sign On implementation

Brute Force

- Threat actor continuously guessing password credentials based on trial and error
- Typically, software assisted or automated
- Control by:
  - Multi-Factor Authentication
  - Compliance with password complexity requirements (i.e., non-dictionary terms)

20

20

Common Attack Vectors – (Continued)

Phishing and Spear phishing

Phishing and Spear Phishing (Targeted)

- Social Engineering technique where the target is contacted by someone posing to be legitimate supervisor, colleague, or business partner
- Control by:
  - Information Security Training and education (at hire and periodically thereafter)
  - Phishing campaigns

21

21

Common Attack Vectors – (Continued)

DDoS

Distributed Denial of Service (DDoS)

- Attacks against networked resources (i.e., data centers, servers) with the intent of limiting availability of the service
- Control by:
  - Content Delivery Network (CDN) – geographically distributed servers
  - Implement DDoS specific protections from cloud providers
  - Firewall and network configurations preventing repeat contact attempts or routing disruption

22

22

Common Attack Vectors – (Continued)

Network, System and Web Application Attacks

Vulnerabilities

- System or network exploit which could grant inappropriate access or permissions to threat actor
- Control by:
  - Patch Management (Operating Systems and key applications)
  - Vulnerability scanning
  - Penetration Assessment
  - Subscription to relevant alerting on new vulnerabilities (i.e., US-CERT)

Missing or Poor Encryption

- Transmitting or storing confidential data without encryption (i.e., "plain text").
- Can be compromised by man-in-the middle attacks (transmission) or gaining unauthorized access to data libraries, databases, files, etc.
- Control by:
  - Common best practices encryption methods – data-at-rest and transport (i.e., TLS, SSL)

23

23

Common Attack Vectors – (Continued)

Network, System and Web Application Attacks

Cross-Site Scripting (XSS) and other web application attacks

- Injecting malicious code into a website which targets the website's visitors
- Control by:
  - Secure Code Development (i.e., OWASP Top-10)

Session Hijacking

- Attacker hijacking the session key assigned to your computer which allows them to access the system without re-logging in
- Control by:
  - Secure Code Development (i.e., OWASP Top-10)

Injection (SQL)

- Malicious code inserted into database programming language which instructs the server to disclose confidential information
- Particular security risk for databases storing Credit Cards, Credentials, or other PII
- Control by:
  - Secure Code Development (i.e., OWASP Top-10)

Man in the Middle

- Attempt to intercept internet traffic in transit
- Most common at public wi-fi spots and networks
- Control by:
  - Encryption of Data in Transit (i.e., TLS, SSL)
  - Most commonly protected through segmentation and enterprise VPN networks
  - Certificate management
  - Trusted access points

24

24

Common Attack Vectors – (Continued)

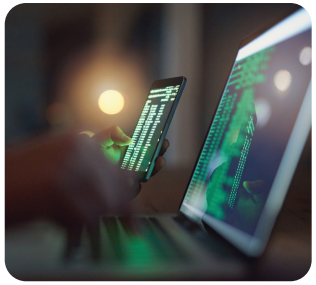
Malware

Malware

Software or programs pretending to be legitimate but action maliciously

Types of Malware

- Trojans
- Spyware
- Adware
- Rootkits
- Ransomware
- Worms
- Keylogger



25

25

Common Attack Vectors – (Continued)

Malware - Ransomware Prevention and Detection

- Back up your data and keep a recent backup off-site, access controlled and logically separated
- Network and host segmentation, zero trust
- Access control and multifactor authentication
- Use anti-malware, web proxy and browser popup protections
- EDR/Anti-Virus/Malware endpoint monitoring
- Web and network proxies
- Information Security Training (be suspicious of unsolicited attachments or links)
- Email filtering (Trojans and malware are often spread via email)
- Maintain current patches (OS, browsers, software, MS Office, plugins if needed, etc.)

26

26

Ransomware

Example Chain of Events (Compromise / Installation)

- RDP, VPN, Vulnerability or phishing Compromise
- Installation of EMOTET and Trickbot (trojans)
- An obfuscated PowerShell script is executed and connects to a remote IP address.
- A reverse shell is downloaded and executed on the compromised host
- PowerShell anti-logging scripts are executed on the host
- Reconnaissance of the network is conducted using standard Windows command line tools along with external uploaded tools
- Lateral movement throughout the network is enabled using Remote Desktop Protocol (RDP)
- Service User Accounts are created
- PowerShell Empire is downloaded and installed as a service
- Lateral movement is continued until privileges are recovered to obtain access to a domain controller
- PSEXEC is used to push out the Ryuk binary to individual hosts
- Batch scripts are executed to terminate processes/services and remove backups, followed by the Ryuk binary

Source: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

27

27

Common Attack Vectors – (Continued)

Business email Compromise (BEC) and (Corporate Account Takeover)

BEC and Corporate Account Takeover

- Attacker gains access to a user's email and leverages the trust and relationships to conduct illicit transactions.
- Protect by:
  - Don't share everything in your social circle
  - Training and awareness
  - Scrutinize all emails, links, mobile downloads and app permissions
  - Implement multifactor authentication,
  - SOD on disbursements with OOB verification,
  - Layered technical security and good accounting controls
  - Restrict authorized disbursements from trusted platforms

Chain of Events

- Targeted spear-phishing campaigns, malware, web or email spoofing
- Infect with malware (credential harvesting)
- Compromise an account(s), harvest information with stealthy execution
- Enumerate disbursement procedures and orchestrate an attack
- Exploitation of trust (without verification)
- Redirect and steal funds

28

28

Shadow IT

Systems and technology used that have not been approved or included in a corporate technology or cybersecurity governance program.

Types of Shadow IT:

- Personal devices
- Cloud storage
- IOT
- Personal email
- Messaging apps
- External media
- Personal printers

29

29

Other Attack Vectors

IoT Hacking

- Embedded device hacking
- Control by:
  - Proper access control
  - Proper physical and logical security
  - Proper segmentation
  - Firmware and system updates
  - Third-Party Diligence

Malicious Insiders

- Disgruntled employees or ex-employees who can expose credentials or confidential information, or unmitigated vulnerabilities
- Control by:
  - Robust Cyber Risk Management Program

30

30

Polling Question #3

- ***When it comes to cybersecurity incident response communication, my organization:***
  1. Unfortunately had to report an incident that lead to a breach
  2. Has had one or more incidents, but has not suffered a breach needing communication
  3. Has never had an incident

3

31

31

Cybersecurity Governance

Cherry Bekaert
Your Guide Forward

32

Cybersecurity Governance

Organization governance models will vary depending on size:

- Board of Directors
- Technology or IT Steering Committee
- Risk committee
- Audit committee

33

33

Cybersecurity Governance

Communication

Needs to be appropriate for the level of organizational governance (know your audience)

Cybersecurity risk needs to be presented as a business risk

Strategy, Compliance, Operational, Financial, Reputational Risks

34

34

Cybersecurity Governance Checklist

- Strategy (objectives, resources, business strategy)
- Governance
- Critical Data and Asset Identification
- Risk Management (include pandemic and remote workforce considerations)
- Vulnerability Management
- Third Party and Supply Chain Risk Management
- Monitoring and Reporting
- Incident Response and Breach Notification
- Awareness and Training

35

35

Cybersecurity Risk Management for Investment Advisers, Registered Investment (Proposed Rule – Q1-2022)

- Builds on SEC Staff Guidance released in 2011 and also on the 2018 Interpretive Release.
- Objective is to increase transparency and consistency around cybersecurity reporting to investors and financial stakeholders
- Increase standardization in the reporting and disclosure of material cybersecurity incidents.
- Identify and prioritize communication efforts related to cybersecurity makeup and practices for investors.
- It specifically includes:
  - A four-business-day notification deadline for reporting material cybersecurity incidents;
  - Mandatory disclosures regarding the board of directors' oversight of cybersecurity risk and individual board members' cybersecurity expertise; and
  - Mandatory disclosures regarding the role of management in addressing cybersecurity risk.
- Information expected to be included on the 10-K and 10-Q filings and where relevant on the Form 8-K (report of unscheduled material events or corporate changes at a company that could be of importance to the shareholders or SEC)
- Information on the form 8k is expected to include
  - When the incident was discovered and whether it is ongoing;
  - A brief description of the nature and scope of the incident;
  - Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
  - The effect of the incident on the company's operations; and
  - Whether the company has remediated or is currently remediating the incident.

Sources: https://www.sec.gov/rules/proposed/2022/33-11028.pdf
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
https://www.sec.gov/news/press-release/2018-22

36

36

Security/Cybersecurity Frameworks & Publications

- AICPA Trust Service Criteria
- NIST CSF
- NIST 800-53, 800-171 – CMMC
- NIST Special Publications
- HIPAA
- FedRAMP / FISMA
- HITRUST CSF
- ISO
- PCI
- FFIEC Cybersecurity Assessment tool
- Information Security Forum
- CSA - Cloud Security Alliance CCM
- ALTA
- Center for Internet Security (Critical Security Controls & Configurations)
- And more…

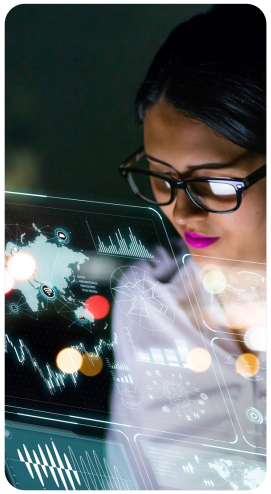
37

37

Incident Response Planning

Cherry Bekaert
Your Guide Forward

38



Objectives of an IR Plan

- Safeguarding of covered and protected information
- Identify an attack
- Contain the damage
- Eradicate the root cause
- Timely and effective restoration of business operations and service level agreements

39

39

Breach Notification Requirements

- State law
- Federal law
- Global requirements (GDPR, etc.)
- Regulatory requirements (ex. HIPAA, CMMC, PCI, PCAOB, etc.)
- Third-Parties (customers, vendors, partners)
- Individuals

40

40

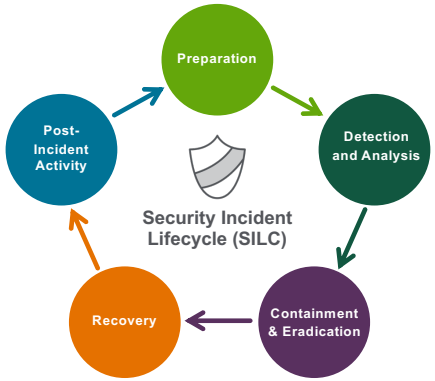
Polling Question #4

- ***When it comes to cybersecurity insurance, my organization:***
  1. Has a comprehensive cybersecurity policy
  2. Has a policy, but I am not sure of the completeness of coverage
  3. Does NOT have a cybersecurity policy, but has other insurance protection (business interruption, crime, etc.)
  4. Does not believe in insurance

41

41

Incident Response Planning



42

42

Key Takeaways

- Stay current on risks and threats
- Know your data (classification and location)
- Cyber Crimes are consistently occurring, and the related costs are increasing.
- Social engineering / spear phishing attacks and will continue to use current events (pandemic, remote work, etc.).
- Use strong authentication practices.
- Question the request. When in doubt contact a manager or IT representative to verify the request.
- Use search engines to navigate to web sites rather then clicking links within emails.
- Incident Response Procedures should be reviewed with all employees.
- Call for verification based on authoritative publications.
- Follow your instincts…

43

43

Key Takeaways (Continued)

- It's a Business Problem
- Stop focusing on "if" we get breached and focus on "when"
- Understand the significance of Executive, Board Level and Audit Committee involvement for Information Security Governance
- Insist on a reasonable level of transparency to the organizations security governance program including risk management and incident response activities
- Stay involved and include information security / privacy governance high level strategic initiatives and performance metrics as regularly reviewed artifacts
- Leverage and benchmark against frameworks
- Use appropriate communication sources
- Govern as you would other business issues
- Ask the question, don't be intimidated by technology terms

44

44

Steven J. Ursillo, Jr.
National Leader, Information Assurance & Cybersecurity
Cherry Bekaert
401.250.5605
sursillo@cbh.com
@StevenUrsilloJr

Cherry Bekaert
Your Guide Forward

45

Cybersecurity Industry Frameworks

National Institute of Standards and Technology (NIST)
NIST Cybersecurity Framework, NIST Risk Management Framework
http://www.nist.gov/

Center for Internet Security (CIS)
CIS Critical Security Controls
http://www.cisecurity.org/

International Organization for Standardization (ISO)
ISO 27000-series publications
http://www.iso.org/

ISACA
COBIT 5 Framework
http://www.isaca.org/

46

46

Additional Resources and Topics

Ransomware Guide and Resources (CISA)

https://us-cert.cisa.gov/ncas/current-activity/2021/05/11/joint-cisa-fbi-cybersecurity-advisory-darkside-ransomware

Common Elements of a Cyber Incident Response Plan

https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf

47

47

Thank you

Cherry Bekaert
Your Guide Forward

48

48