CYBER THREATS & SOLUTIONS – WHAT SCHOOL LEADERS NEED TO KNOW

Jake Omann
Mohammad ElSawaf

March 22, 2023

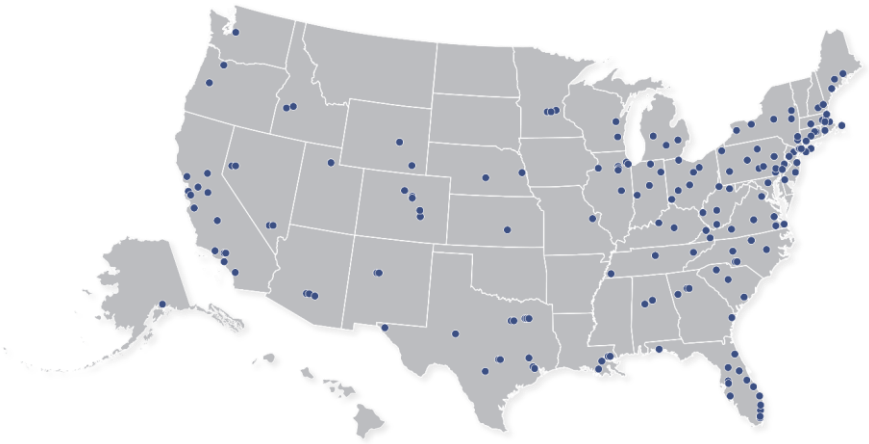
usi.com

Agenda

- Threat Landscape
- Cyber Market Update
- Cyber Underwriting Focus
- Building a Solution – Cyber Insurance
- How USI Can Help

USI Brings National Capabilities & Local Expertise

USI is a pre-eminent national insurance brokerage and consulting firm with more than 200 local offices connected across the U.S. and a leading market position in all core businesses.



Commercial P&C | Employee Benefits | Personal Risk | Programs | Retirement Consulting

- Over $2B in U.S. Revenue
- More than 100 years of brokerage experience through our acquired agencies
- Broad and deep knowledge based on the shared expertise and experience of 8,000+ professionals across industry verticals
- Over 500,000 clients served across all lines of business with superior account service and targeted solutions
- Proprietary Risk Management process, USI ONE Advantage®, delivers superior client solutions with financial impact
- Dedicated School Practice

School Districts Threat Profile

ATTACK VECTORS

Loads of data
And in most cases these days, nearly every computer system that stores data—from gradebooks to door locks to salary information—relies on some sort of online network that is capable of being hacked.

Heavy Reliance on Technology
During the pandemic, millions of digital devices for remote learning, set up WiFi hotspots around communities for students to access, and dramatically increased the use of online programs and apps for instruction.

Vendor/Third-Party Remote Access
Remote vendors with the ability to connect into OT systems without proper security controls can spread infections into OT

Insider Threats
Disgruntled employees, students, contractors, and vendors with access and accounts can use these to compromise systems

ATTACKER MOTIVATIONS

Monetary Gain
Many recent forms of attack, including ransomware, are motivated by attackers seeking financial gains through the sale of compromised data or through ransoms of critical computer systems

Geopolitical
In a complex global environment, many can be nation-state sponsored or sanctioned

Social/Political (Hacktivism)
Cyber attacks designed to send a message or elicit change to a particular cause or industry can be motivated by a particular social or political belief

Schools also grapple with “class invasions,” (also known as “Zoombombing” tp disrupt class or “Meeting invasions,” often not for any specific reason other than to irritate district officials.

Top 4 Cyber Threats

DATA BREACH

Protected or confidential data has been viewed, stolen, or used by an unauthorized individual.

As of 2022, the global average cost per data breach amounted to **4.35 million U.S. dollars**, an increase from 4.24 million U.S. dollars in the previous year.

Cost of a data breach 2022 | IBM

BUSINESS INTERRUPTION

Attack that directly or indirectly causes business interruption or network degradation, incl. recovery costs.

Average costs recovery and downtime following a cyber incident more than doubled in the past year growing from $761,106 to $1.85M. The increase is attributed in part to ransom demands, denial of service attacks, and rising supply chain attacks.

https://www.propertycasualty360.com/2021/10/15/cyber-losses-are-driven-by-business-interruption-recovery-costs/

CYBER EXTORTION

Cyber attack or threat of an attack against an organization coupled with a demand or request for money or other actions to avert or stop the attack.

Between the first and second quarters of 2022, the number of ransomware attacks saw an 18 percent increase, going from nearly 130 million incidents to approximately 106 million incidents worldwide.

https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide/

SOCIAL ENGINEERING

"Business Email Scam" or "Phishing" uses deception to manipulate individuals into divulging confidential or financial information.

Social Engineering scam losses jumped 20% to $4.2B in 2020 Remote workforces may be more susceptible to this type of attack. Email, SMS texting attacks ("smishing") and even phone calls with a live person ("vishing") are attack vectors.

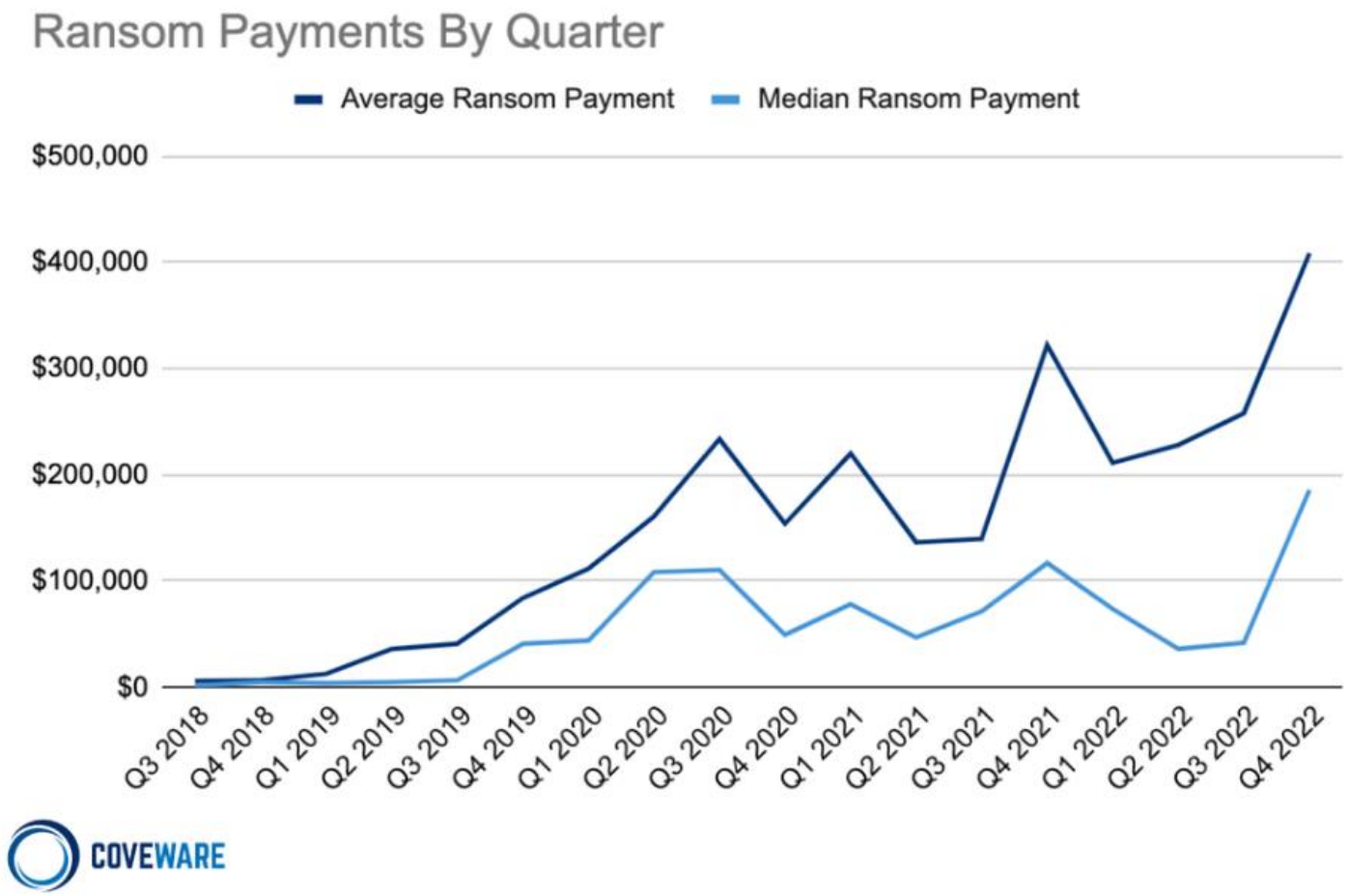
https://pdf.ic3.gov/2020_IC3Report.pdf

Ransomware attacks are expensive

- Demands are larger
- Change in tactics:
  - Hackers “professionalized”
  - lay the “groundwork”
- “Double Extortion”
  - Release data to public
  - Encrypt files and operating systems
- More difficult to extract the malware from affected systems
- Average downtime is 21 days
- Industries targeted:
  - healthcare
  - government
  - professional services (increase)

*cases worked by Palo Alto Networks

Data breach events are expensive



Data breach events are expensive

Breach Notification Costs

Data breach events are expensive

- It's your data, even if you outsource the storage to the cloud
- If you have a breach, call in the experts (attorneys, forensics) early.
- Have a Breach Response Plan, and follow it carefully:
  - Maintain Attorney Client Privilege
  - Identify the source and extent of the breach
  - Address both the legal and ethical obligations
  - Be careful with communication and customer questions
  - Document everything
- Do a detailed post-mortem; Don't try to go back to "normal" without evaluating what needs to be changed

"Top 10"Cyber Underwriting Focus Areas in 2023

1. **PRIVILEDGED ACCESS MANAGEMENT**
   - In use and for whom? Who is vendor?
   - Complexity levels and Check In/Out?
2. **MONITORED END POINT DETECTION AND RESPONSE (MDR) & EXTENDED DETECTION AND RESPONSE (XDR):**
   - Vendors used + maturity level (note, this must be tied to #3)
3. **24/7 NETWORK MONITORING AND SECURITY OPERATIONS CENTER (SOC):**
   - Internal or external (via MSSP)?
   - 24/7 centralized w/logs and reports + action/remediation?
4. **NETWORK BACK-UPS:**
   - Encrypted? Immutable? Is MFA required for access?
   - Location: Off site? Co-location? Air-gapped?
   - Frequency and Security of back-ups and cadence
5. **NETWORK SEGMENTATION:**
   - Critical systems segmentation in place?
   - EoL (End of Life) / EoS (End of Support) strategy?
   - Process for monitoring and preventing lateral movement?
   - Patching and patching cadence? Especially for critical risks.
6. **"VULN" or "CVE" Alert/Hunting teams**
   - In use? internal or external?
7. **DOMAIN ADMINISTRATOR ASSIGNMENT/OVERSIGHT**
   - REVIEW CADENCE?
8. **NUMBER OF SERVICE ACCOUNTS**
9. **EMAIL SECURITY – DKIM/DMARC/SPF?**
10. **TPRM Control (Third Party Risk Mgmt)**

Cyber Underwriting focus notes:

Cyber Security "Table Stakes" – 2023:

- MFA for ALL: Email, Privileged Accts, Remote
- TRUE MFA – tokens, push notices – not certs
- Records – located, number and protections?

"Headline" items: UW's may inquire about emergent "headline" cyber risks

Biometric– specific amount and type of any employee or customer Biometric information collected and where it's collected.

Building a Solution – Cyber Insurance

Building Block #1

Liability Costs

Trigger: Liability costs when someone sues you or makes a demand as a result to.

Coverage Included:

- Privacy Liability
- Network Security Liability
- Media Lability

Building Block #2

Breach Response Costs/ Mitigation Costs

Trigger: Mitigation and Compliance Costs

Coverage Included:

- Notification Costs
- Forensic Costs
- Privacy Regulatory Costs
- Payment Card Industry/Data Security Standards
- Public Relations Expenses

Building Block #3

Direct Costs

Trigger: Direct costs to your business as a result of a security failure/system failure

Coverage Included:

- Cyber Extortion/Ransomware
- Network Interruption/Extra Expense
- Contingent Network Interruption/Extra Expense
- Bricking Coverage
- Data Reconstruction
- Reputational Harm BI/EE

Typical Cyber Exclusions

Exclusions include but are not limited to:

- Coverage best addressed in another insurance policy
- Intentional Acts Exclusion “Conduct Exclusion”
  The intent is to protect the entity against the acts of rogue or uninformed employees.
- Certain actions against public policy and consumer protection laws
  - FTC Federal Trade Commission
  - ERISA (Employee Retirement Income Security Act)
- Prior Knowledge of prior acts…the building is burning and now we need insurance. The intent is of course to protect the entity against unforeseen events
- Bodily Injury/Property Damage
  - Carve-backs for Privacy/Media/Bricking Events/Professional Services
- Infrastructure, Act of War (physical) and Nuclear
- **Pixel – Wrongful Collection (trending)**

Coverage Trends – Language to look for

- Ransomware limitations: sub-limits/co-insurance/exclusions
- Dependent Business Interruption/”Supply Chain”: sub-limits or removal of coverage
- Specific Event Exclusions (i.e., Log4j, Microsoft Exchange Server)
- Systemic Events Exclusions : sub-limits/co-insurance/exclusions
- Music Copyright Exclusions
- Coverage limitations specific to individual risk

Insurance is available, but market is challenged

Reactions of Cyber Insurers

- Raising rates
- Raising deductibles
- Introducing co-insurance
- Reducing offered limits
  - overall for companies buying $10M or more limits
  - line-item coverages (e.g., business interruption, ransomware)
- Much more vigorous underwriting
  - Demanding additional security (e.g., Multi-Factor Authentication)
  - Requiring specific software
  - Performing their own penetration tests
  - Questions about exposure to SolarWinds, Microsoft Exchange
- Exiting Cyber market altogether

USI Answerlytics – Putting It All Together

Risk Identification

- Assess cyber security maturity level
- Regulatory exposure analysis
- Managed security services
- Board level understanding of threat response
- Cyber risks specific to M&A activity and integration

Cyber Answerlytics Risk Mitigation

- USI's network of Answerlytics Curated Providers (ACPs) address clients' key vulnerabilities
- ACPs provide prioritized access to cutting- edge risk management solutions at discounted pricing
- ACPs help clients improve cyber hygiene before incidents occur

Risk Transfer

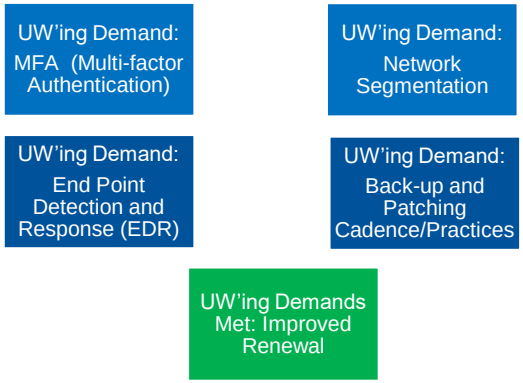
- Assess Cyber Security Maturity level
- Regulatory Exposure Analysis
- Managed Security Services
- Board Level Understanding of Threat Response
- Cyber risks specific to M&A activity and integration

CYBER

Cyber Risk Control with Answerlytics™

Improve client risk control, reduce the cost of risk transfer, and address contract requirements with USI Answerlytics, a trademarked solution developed by USI.

- Answerlytics curated providers (ACPs) address clients' key vulnerabilities and associated cyber underwriting (UW) demands.
- ACPs offer prioritized access to cutting-edge risk management solutions at discounted pricing of services (typically 20%+).
- ACPs help clients improve cyber hygiene via cyber risk control pre-event – USI has solved for broker facilitated Cyber knowledge and solution distribution vs. carriers, benefiting clients.



Impact and Benefits

- Improved Renewal terms
  - Coverage, retention, restrictions
- Streamlined cyber insurance procurement process
- USI-provided data and analytics as a result of data sharing agreements with ACPs
- Improved cyber risk knowledge: regulatory exposures, cyber-linked supply chain risks, ransomwarerisks
- Improved Vendor and M&A negotiations

Thank You!

Contact Information

Jake Omann
Jake.Omann@usi.com

Mohammad ElSawaf
Mohammad.ElSawaf@usi.com

USI Cyber Glossary

CYBER RISK CONTROL TERMS AND CRITICAL CONCEPTS

- Access Control
  - Measures taken to limit access to something, such as an IT system, program, or information. For a shared hard drive, permissions settings can be changed so that only certain user accounts can access files on that hard drive. For physical access, this includes key fobs or passes to unlock doors.
- Administrator
  - A person in an organization who is responsible for managing a computer system or network (in whole or a portion).
- Advanced Persistent Threat (APT)
  - A sophisticated security breach that enables an attacker to gain access or control over a network for an extended period, usually without the awareness of the system's owner.
- Air Gap
  - A security measure wherein computer systems or networks are not connected in any way to any other devices or networks. The goal is to ensure total isolation of a given system, most importantly physically, from other networks including the internet. Data can only be transferred by connecting a physical device to air gapped device - no lateral movement possible is the target. A cyber underwriter's focus is on air gapped backups - copies of network data completely separate physically from any network connections including internet access.
- Asset
  - Data, devices, or other components of the network environment that support cyberactivity.
- Asset Management
  - Developing, operating, maintaining, upgrading, and disposing of Information Technology (IT) assets throughout their lifetime. Asset Management may also keep track of assets and their support lifecycles.
- Authentication
  - The process of identifying a user via a password, PIN, and/or other means. Up-to-date Authentication uses multiple factors, such as a password in conjunction with something the person possesses (Smartphone, VPN fob, etc.), or something personal (biometric scan involving a fingerprint, eye scan, voice recognition, etc.).
- Authorization
  - The security mechanism determining and enforcing what authenticated users are authorized to do within a computer system.

- Backup
  - The process of creating and storing copies of data and network information that can be used to protect organizations against data loss. A proper backup copy is stored in a separate system or medium from a network, or "air gapped" (i.e., physically disconnected) from the primary data and network to protect against the possibility of data loss.
- Botnet
  - A collection of third-party computers that have been compromised by malicious code to run malware; an attacker is then able to remotely take advantage of the computer systems' resources to perform illicit or criminal actions.
- Bring Your Own Device (BYOD)
  - A company's security policy that dictates whether employees can bring their own devices into the work environment, connect them to the company network, and allow interaction with company resources via employee mobile phones, pads, laptops, etc.
- Business Continuity Plan (BCP)
  - A business plan used to resolve issues that threaten core business functions during a cyber event.
- Cloud Computing
  - The delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.
- Command and Control (C&C) Server
  - A server controlled by a bad actor (hacker, malware controller, etc.) which is used to send commands and receive exliltrated data.
- Common Vulnerabilities and Exposures (CVE)
  - The entries that make up the database of publicly known/disclosed information security "vulnerabilities" (example - a software code error) and "exposures" (example - a software configuration error) as defined by U.S. Dept of Homeland Security (DHS). Standardization o f these known CVEs is meant to allow for quick reference and ability to diagnose threats for underwriting across industries and networks.
- Computer Network Defense (CND)
  - The establishment of a security perimeter and internal security requirements with the goal of defending a network against cyberattacks, intrusions, and other violations. A CND is defined by a security policy and can be stress-tested using vulnerability assessment and penetration testing measures.
- Connection Exhaustion
  - A type of Denial of Service (DoS) attack that repeatedly makes connection requests to a target to consume all system resources related to connections, which prevents any other connections from being established or maintained.

- Cyber Attack/Incident
  - Any attempt to violate the security perimeter of or the privacy of data held by, an organization, group or individual. Cyber-attacks take many forms, but most are for the purpose of gathering and exfiltrating information (including private data), damaging business processes, monitoring targets, or using compromised network resources to support attacks against other targets.
- Crypto Jacking
  - The unauthorized use of a computer network to mine cryptocurrency through use of malware.
- Cyber Security
  - The effort to design, implement and maintain security for an organization's network. An organization's cybersecurity should be defined in a security policy, verified through evaluation techniques (See "Penetration Testing "and "Vulnerability Assessment"), revised against standards, and updated and improved as the organization evolves and as new threats are discovered.
- Data Breach
  - Includes but not limited to the disclosure of confidential information, access to confidential information, and unauthorized destruction of data assets. Generally, a data breach results from the unauthorized accessing of personal and/or health data by external entities without authorization.
- Data Loss
  - Data Loss occurs when protected data, such as personal and health data, is lost by the responsible party and possessed by unauthorized entities. An example would be when a storage device is lost or stolen containing personally identifiable (PII) or personal health (PHI)information. Also known as "Data Leakage."
- Data Loss Prevention (DLP)
  - A collection of security mechanisms that aim to prevent the occurrence of data loss and or data leakage. DLP seeks to prevent cyberbreach occurrences through various techniques, such as by placing strict access controls on resources, blocking the use of email attachments, preventing network file exchange to external systems, blocking cut and paste, disabling use of social networks, and encrypting stored data.
- Data M i n i n g
  - The activity of analyzing and/or searching through data to find items of relevance, significance, or value. The results of data mining are known as meta-data.
- Data T h e f t
  - The act of intentionally stealing data. Data theft can occur via physical or electronic data loss.
- Decrypt
  - The act that transforms ciphertext (the random form of data that is produced after encryption) back to its original plaintext or cleartext form. Decryption is a key ransomware concept.

- Distributed Denial of Service (DDoS)
  - An attack that attempts to block access to and use of a resource via overloading a Server with requests in a short period of time.
- Digital Footprint
  - Someone's unique set of digital activities/actions that can be traced on the internet or on digital devices.
- Digital Forensics
  - The means of gathering digital information to be used as evidence in a legal procedure. Digital forensics focuses on gathering, preserving, and analyzing the data from a computer system and network.
- Disaster Recovery Plan
  - A plan that is like an incident recovery plan but designed to help an organization recover from larger disaster level incidents.
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
  - An email security protocol that uses Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to determine the authenticity of an email message.
- DomainKeys Identified Mail (DKIM)
  - Allows senders to associate a domain name with an email message, thus vouching for its authenticity. S ender creates the DKIM by "signing" the email with a digital signature. The "signature" can be found in the message's header.
- Employee Training Program
  - Cybersecurity training to protect employees and the company against cyberattacks. The focus is on employee awareness of current security threats, such as spam, phishing, malware, ransomware, and social engineering. Required by underwriters.
- Encode
  - The act of transforming plaintext or cleartext (a.k.a. original form) into ciphertext (using symmetric encryption algorithm).
- Encryption
  - A method of protecting information or data by encoding it. If data is encrypted, it can be read only by having the correct key or password. Encryption is often recommended for sensitive data.
- Encryption Key
  - The secret number value used by a symmetric encryption algorithm to control the encryption and decryption process. The longer the key, the more security it provides.

- Endpoint Application Isolation and Containment Technology
  - A form of zero-trust endpoint security. Instead of detecting or reacting to threats, it enforces controls that block and restrain harmful actions to prevent compromise. App containment is used to block harmful file and memory actions to other apps and the endpoint. App isolation is used to prevent other endpoint processes from altering or stealing from an isolated app or resources.
- Endpoint Detection and Response (EDR)
  - Also known as "endpoint threat detection and response, "this process centrally collects, monitors, analyzes, and responds to comprehensive endpoint data across an entire organization to alert/eliminate potential threats. Common providers include CrowdStrike Falcon Endpoint Protection, Sentinel One, Carbon Black Cloud, and Cisco AMP.
- External Penetration Testing
  - A security assessment of the perimeter security systems that replicates the activities of real hackers. This test typically operates without access to a targets systems or networks.
- Firewall
  - A security tool (hardware or software) that is used to filter network traffic.
- Flooding Attack
  - A type of Distributed Denial of Service (DDoS) attack that sends massive amounts of network traffic to the target, overwhelming the ability of network devices and servicers to handle the raw load.
- Forensic Activities
  - Measures taken to collect or preserve evidence. In the context of cybersecurity, forensic activities help ensure the preservation of information that may be needed for an investigation and prevent tampering or accidental modification.
- Hacker
  - A person who has knowledge and skill in analyzing program code for computer systems, and who can modify a system's functions or operations and alter its abilities and capabilities. Hackers may be ethical and authorized or malicious and unauthorized and can range from professionals who are skilled programmers to those who have little knowledge of the specifics of a system but who can follow directions (aka, "Script Kiddies").
- Hacktivism
  - Attackers who hack for a cause or believe rather than for some form of personal gain. Hacktivism is often viewed by attackers as a form of protest or as a way of fighting for their perceived right or justice. This activity is illegal when a victim's technology or data is abused, harmed, or destroyed.
- Incident Recovery Plan
  - A plan designed to aid in recovering from an incident. It differs from an Incident Response plan in that it is focused on reversing the effects of an incident after it has happened. Such a plan may repair or limit reputational damage, depending on whether the incident affected other parties (such as customers of business partners).

- Incident Response Plan
  - A set of instructions that should be followed in the event of a security incident to help contain or prevent adverse impacts to IT systems or their data. These plans can address different scenarios such as (but not limited to) the loss of data, service outages, or compromise of IT systems.
- Internet Connection Sharing (ICS)
  - Allows multiple computers to connect to the internet using the same internet connection and IP address.
- Internet of Things (IoT)
  - The internet connectivity of physical objects such as vehicles, devices, buildings and electronics and the networks that allow them to interact, collect, and exchange data.
- Malware
  - A computer program that is covertly placed onto a computer for electronic device with the intent to compromise the confidentiality, integrity, or availability of data, applications, or operating systems. Malware commonly includes viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and some forms of adware.
- Multi-Factor Authentication (MFA)
  - An authentication method in which a user is granted access to a website or application only after successfully presenting three or more "factors" or pieces of evidence to an authentication mechanism: knowledge (password), possessional item (phone, key), and/or biometrics information (fingerprints, facial scan, retina/iris scan, etc.).
- Network
  - An information system implemented with a collection of interconnected components, such as computers, routers, hubs, cabling, and mobile devices.
- Network Segmentation
  - Splitting a network into sub-networks by creating separate areas that are protected by firewalls configured to reject unnecessary traffic. Network segmentation minimizes the harm of malware (and other threats) by isolating it to a limited part of the network.
- Network Segregation
  - Separating critical networks from the internet and other less sensitive networks. Network segregation can be used in combination with network segmentation.
- Next-Generation Anti-Virus (NGAV)
  - Software that uses predictive analytics driven by machine learning, artificial intelligence, and threat intelligence to detect and prevent malware and exploit kits, identify malicious behavior, and respond to new and emerging threats that previously went undetected.
- Patches/Patching
  - Software released by developers to fix software bugs and vulnerabilities (known as updating or patching software) to help prevent attacks on an IT system. Patching Cadence is sought by underwriters particularly for critical risks.

- Patching Cadence
  - How often an organization reviews systems, networks, and applications for updates that remediate security vulnerabilities and how quickly these items can be installed.
- Penetration Testing
  - A penetration test, also called apentest or ethical hacking, is cybersecurity technique organizations use to identify, test, and highlight vulnerabilities in their security posture. Penetration tests are often carried out by ethical hackers. Underwriters will require cadence of testing.
- Phishing
  - The process by which scammers send fake emails, usually personalized for more efficient attack, requesting sensitive information or containing links to bad websites in the attempt to trick individuals into sending money or stealing information.
- PowerShell
  - A powerful cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. It is used by IT departments to run tasks on multiple computers in an efficient manner. It can be exploited and threaten entire organizations given its reach in the network.
- Privileged Account Management software (PAM)
  - Allows organizations to secure privileged user credentials in a centralized, secure vault (a password safe). To qualify for inclusion in the Privileged Access Management category, a product must allow administrators to create and provision privileged access accounts, offer a secure vault to store privileged credentials, and monitor/record/or log user actions while using privileged accounts.
- Protective DNS service
  - DNS protection (also known as DNS filtering) provides an additional layer of protection by blacklisting dangerous sites and filtering out unwanted content. It can also help detect and prevent malware that uses DNS tunneling to communicate with a Command and Control (C&C) server.
- Ransomware
  - A type of malware that prevents or limits users from accessing their system, usually by locking the users' files until a ransom is paid. More modern ransomware malwares encrypt certain file types on infected systems and force users to pay the ransom through certain payment methods (i.e., cryptocurrency) to obtain a decryption key.
- Remote Desktop Gateway (RDG)
  - Enables authorized users to connect to virtual desktops, remote app programs, and sessions-based desktops over a private network or the internet. No longer seen as secure by underwriters
- Remote Desktop Protocol (RDP) Connections
  - A proprietary protocol developed by Microsoft that provides a user with a graphical interface to connect to another computer over network connection. The Microsoft RDP provides remote display and input capabilities over network connections for Windows-based applications running on a server. No longer seen as secure by underwriters.

- Risk Assessment
  - A process in which risks in an IT system and corresponding potential impacts are identified to an organization. Once the risks have been identified and assessed, measures can be developed and implemented to address them.
- Router
  - A device that allows communication between different networks. Routers determine the best path for forwarding data to its destination.
- Security Information and Event Management System (SIEM)
  - A subsection within the field of computer security, in which software products and services combine security information management and security event management to provide real-time analysis of security alerts generated by applications and network hardware.
- Security Operations Center (SOC)
  - A centralized unit or group that deals with security issues on an organizational and technical level. 24/7 functionality is sought by underwriters.
- Sender Policy Framework (SPF)
  - An email-authentication technique that is used to prevent spammers from sending messages on behalf of a particular domain (or "spoofing" the domain).
- Software Support Lifecycle
  - The period in which programs or applications are maintained by their developers (creators/manufacturers). During the lifecycle, the creators/manufacturers will release updates to fix security issues. When software support is no longer available and updates/patches are no longer released, software can become more vulnerable to attacks as it is at 'End of Life" or "End of Support."
- Spyware
  - Software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
- System Development
  - A process to create and implement a hardware or software system. This process involves planning, designing, implementing, and maintaining the system.
- Trojan Horse
  - A type of malware that downloads disguised as a legitimate program.
- Two Factor Authentication
  - Accessing an account or information by using two methods. Usually, the first method is the computer password. The second method may include sending a code to a cell phone (most common), inserting a badge/pass into a computer, connecting via a special USB key, or using fingerprint scanners.

- Virtual Private Network (VPN)
  - A virtual network built on top of existing networks that can provide a secure communications mechanism for data and Internet Protocol (IP) information transmitted via the virtual network.
- Vulnerability
  - A flaw that can be exploited during an attack. The term is commonly used when talking about flaws in software but can refer to flaws in many other aspects of business, such as processes, policies, or physical defenses. Hackers can exploit a vulnerability in software by taking over a computer, viewing or changing confidential information, or compromising a computer in other ways. When vulnerabilities are discovered, developers are likely to issue patches/updates to fix them and stop adverse effects. Also known as "Vuln" or "Lulz Vuln,"- reports on vulnerability scans will be provided by many underwriters and remediation will be required.
- Vulnerability Management Tool
  - A cloud service that provides instantaneous, global visibility into vulnerabilities and threats against IT systems. An ongoing process that includes proactive asset discovery, continuous monitoring, mitigation, remediation, and defense tactics. Common Providers: Qualys, InsightVM/Rapid7, Nessus/Tenable
- Vulnerability Assessment
  - A review of security weaknesses in a network which can be conducted at various times, complexities, and targets.
- Zero Trust
  - The Zero Trust Security Model (also, Zero Trust Architecture, Zero Trust Network), describes an approach to the design and implementation of It systems. The main concept behind zero trust is "never trust, always verify," meaning that devices should not be trusted by default.

USI **ONE Advantage®**
A set of client customized, actionable, measurable solutions with bottom line impact to your business through cost reduction and coverage enhancement resulting in an improved Total Cost of Risk and Employee Benefit trend advantage.

THANK YOU