Cyber Risk Management:
Threat Landscape & Mitigation

Prepared for: Wespath Conference Forum

17 March 2022

Agenda

- Who is Aon Cyber Solutions / Stroz Friedberg
- Overview of Cyber Insurance Coverage
- Current Cyber Threat Landscape
- Current Cyber Insurance Market Update
- Cyber Insurance Underwriting Focus
- Cyber Threat Mitigation Efforts
- Q&A

Aon Cyber Solutions

Our Experience and Qualifications

Aon's Cyber Solutions specializes in ***holistic cyber risk management***.
We approach your cyber exposure with a multifaceted solution: proactive cyber security services, risk transfer, and incident response services.

Cyber Solutions

AON Empower Results®

Recognized leader in risk management and cyber insurance solutions

STROZ FRIEDBERG an Aon company

Global leader in incident response, digital forensics, eDiscovery, investigations, and proactive security advisory services

GOTHAM DIGITAL SCIENCE A STROZ FRIEDBERG COMPANY

Specialists with deep and recognized experience in security testing, application security, code reviews, and red teaming

CYTELLIGENCE

Specialists incident response, digital forensics, eDiscovery, and security training

Aon's Cyber Solutions

More than **3,000** Total Clients

$939 million* Premium Dollars placed per year
*U.S. Premium

90% of highest profile breaches

Aon's Cyber Solutions | Full-Spectrum Cyber Risk Management

Our Unique Value

Security Advisory	Security Testing	Intelligence	Quantification	Broking	Digital Forensics & Incident Response	Investigations	eDiscovery
Identifying your security weaknesses	**Illuminating your systems' vulnerabilities**	**Using knowledge to empower**	**Optimizing your total cost of risk**	**Securing your future**	**Solving your cyber events**	**Uncovering the facts**	**Navigating the complex issues**
Evaluate and remediate your vulnerabilities, determine your readiness to respond, and improve your organization's cyber resilience.	Leverage real-world testing and simulations to help you better understand your weaknesses and strengthen your defenses.	Help protect your organization by applying traditional investigative techniques to the digital environment.	Model cyber loss scenarios and stress test your current insurance limits to enhance your risk financing strategies.	Protect your organization from the financial impact of a cyber incident.	Respond to the incident, create an investigation strategy, contain the incident while preserving evidence, and confidently communicate with your stakeholders	Perform complex financial investigations, forensic accounting, and compliance assessments.	Benefit from professional guidance through ever-changing technical and legal challenges.
See your company like never before.	*Clear your way for peace of mind.*	*Protect your organization's brand.*	*Strategize for your company's future.*	*Know it's not one size fits all.*	*Find the smoking gun.*	*Get back in business.*	*Bring order to the disorder.*

Our People

Protectors and Problem Solvers

- Forensic computer analysts
- Penetration testers
- IT security engineers
- Information security analysts
- Security architects
- Former CISOs
- Fraud examiners
- Security risk consultants
- Investigators
- Criminologists
- Forensic accountants
- Governance & risk mgmt. professionals
- Privacy professionals
- Claims advocates
- Evidence Technicians
- Brokers
- CPAs

Oath Takers

- Former law enforcement*
- Former prosecutors
- AM Law 100 former partners

More than the Sum of Our Parts

- Former Big 4 Professionals
- Actuaries
- Statisticians
- Data analysts

* Includes former Head of the Cyber Division at FBI Headquarters and former founder of the FBI's computer crime squad in New York

Cyber Insurance Coverage

Market Standard Cyber Coverages Overview

- Network Business Interruption
- System Failure
- Dependent Business Interruption / System Failure
- Cyber Extortion
- Digital Asset Restoration

- Privacy and Network Security Liability
- Privacy Regulatory Fines and Penalties
- Media Liability
- PCI Fines and Penalties
- Breach Event Expenses

Operational Risk Elements of Cyber Insurance Coverage

- **Network Business Interruption -** Reimbursement coverage for the insured for lost net income caused by a network security failure, as well as associated extra expense. Retention and waiting periods are negotiable
- **System Failure -** Expands coverage trigger for business interruption beyond computer network security failure to include any system failure
- **Dependent Business Interruption/Dependent System Failure -** Reimbursement coverage for the insured for lost income caused by a network security failure of a business on which the insured is dependent, as well as associated extra expense. Retentions and waiting periods are negotiable.
- **Cyber Extortion -** Reimbursement coverage for the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.
- **Digital Asset Restoration -** Reimbursement coverage for the insured for costs incurred to restore, recollect, or recreate intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a network security failure

Privacy & Network Security Risk Elements of Cyber Insurance Coverage

- **Privacy and Network Security Liability –**
  - Privacy Liability**:** Liability coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential third-party corporate information, whether or not due to a failure of network security. Coverage may include: unintentional violations of the insured's privacy policy, actions of rogue employees, and alleged wrongful collection of confidential
  - Security Liability: Liability coverage for defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus

- **Privacy Regulatory Fines and Penalties -** Liability coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage includes fines and penalties where insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered

- **Media Liability -** Liability coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website only to all content in any medium

- **PCI Fines and Penalties -** Coverage for a monetary assessment (including a contractual fine or penalty) from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an "Acquiring Bank") in connection with an Insured's non-compliance with PCI Data Security Standards

- **Breach Event Expenses -** Reimbursement coverage for the insured's costs to respond to a data privacy or security incident. Policy triggers vary but are typically based on discovery of an event, or a statutory obligation to notify consumers of an event. Covered expenses include computer forensics expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, call centers, and consumer credit monitoring services

Current Cyber Threat Landscape

5 Myths About Ransomware

1. My business is not a ransomware target

Healthcare institutions, retailers, banks, municipalities and larger organizations are often prime ransomware targets, but all businesses, of all sizes, are in the crosshairs of threat actors,[4] who will often choose the easiest path to achieve their goals – attacking vulnerable companies that lack cyber defense and preparedness.[5] That low-hanging fruit is often small and medium-sized businesses. Indeed, according to one estimate, 80% of ransomware incidents affected companies with fewer than 1,000 employees, and 60% of those firms had revenues of less than $50 million.

Further, more frequent and more severe attacks on small and medium-sized businesses are what's helping to drive the increase in premiums being seen in the cyber insurance market these days. That's why it's critical for smaller businesses to ensure they have security measures in place such as multi-factor authentication on password-protected systems, control over who has access to sensitive information, and incident response plans that map out the steps the company should take to recover from an attack.

2. It's only about data backup and encryption

As attackers have become more sophisticated, the backup of data and encryption is no longer enough, in fact threat actors are now exploiting data backups to put further pressure on victims. Threat actors are:

Encrypting back-up data, to prevent restoration of information in lieu of paying the ransom.

Capturing sensitive data, holding it as hostage and threatening to release it to the public if a ransom is not paid.

Should an attack occur, it is crucial that pre-arranged cyber professionals are engaged to thoroughly check what data may have been accessed by threat actors, as well as screen data back-up systems to identify and remove suspicious malware.

5 Myths About Ransomware (cont.)

3. Ransomware losses are limited to ransom payments

According to a survey by security firm Sophos, the global average cost to remediate a ransomware attack is $761,106—and paying the ransom actually doubles that cost to an average of $1.45 million.[6] But the bigger impact for most organizations is the downtime and lost productivity associated with a ransomware attack. Business interruption losses have accounted for 60% of cyber insurance claims in the past five years.[7] Additionally, 70% of ransomware attacks now involve the threat to leak sensitive data, which could cause additional expenses to the company from data breach standpoint, including potential costs associated with complying with state notification laws as well as privacy-related fines and penalties and much higher monetary and reputational losses.

4. Security software is enough protection

Security software alone will not protect an organization. What often happens is that companies aren't pulling all the levers on software, which results in gaps where threat actors can work around the software. To protect against this, companies should create a cybersecurity culture that provides guardrails so that people automatically think twice before opening an email or pause before clicking on an attachment from an unknown sender. Ultimately, it's every employee's job to protect the organization.

5 Myths About Ransomware (cont.)

5. Threat actors attack immediately

Attackers are getting increasingly good at waiting, and often are in company systems for months before they pull the trigger on an attack. Many of them use strategies that plan a bigger attack by starting with small disruptions and learning from them. And depending on what they're looking for, the more specific—such as going after government entities—the more they're willing to wait for the ideal time to strike or to try a range of techniques until they find the weak spot in an organization.

At a very minimum, organizations should have risk mitigation strategies in place, including guidelines for systems access and employing multifactor authentication.

[1] Coveware. Why Small and Medium-sized Professional Service Firms are a Big Target for Ransomware Attacks

[2] Bitfender's Mid-Year Threat Landscape Report 2020, page 1

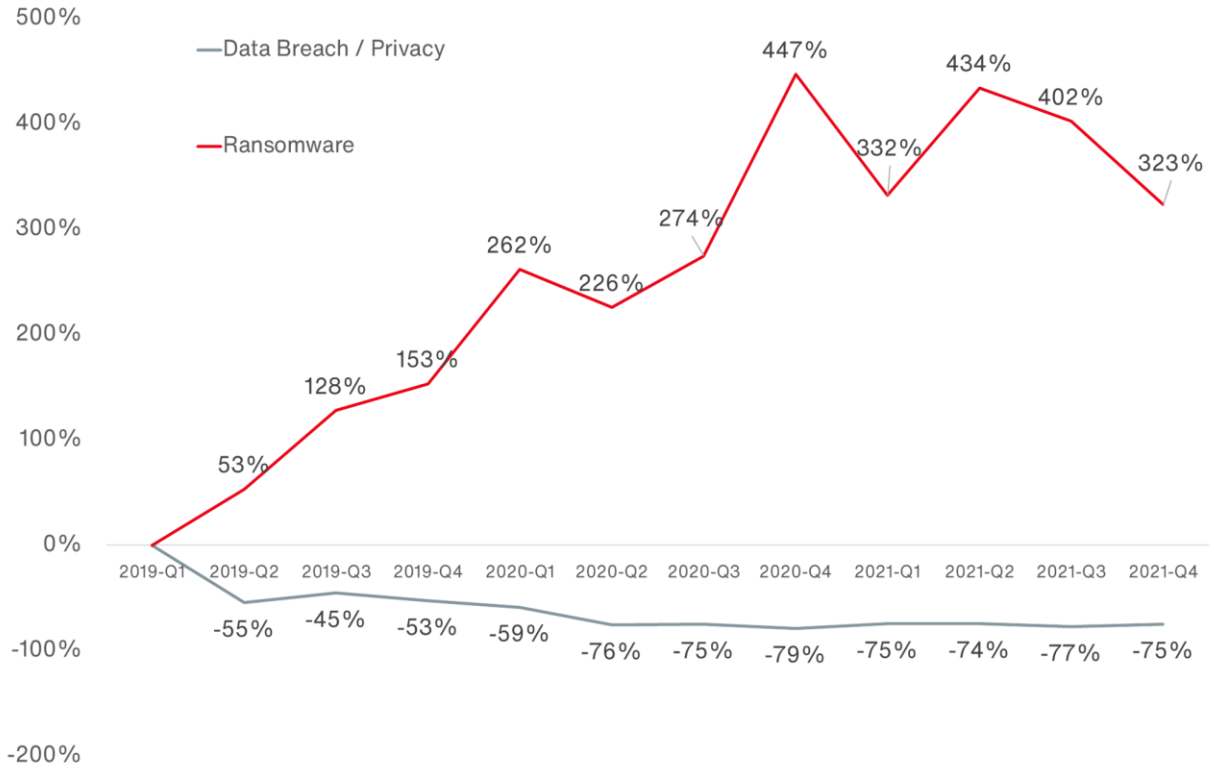
[3] [4] Coveware. Ransomware Marketplace Report, August 3, 2020

[5] The Ransomware Epidemic

[6] The State of Ransomware

[7] Business interruption drives 60% of cyber losses: Allianz

Cyber Incident Rates Over the Past 12 Quarters
(Percent change relative to Q1 2019)



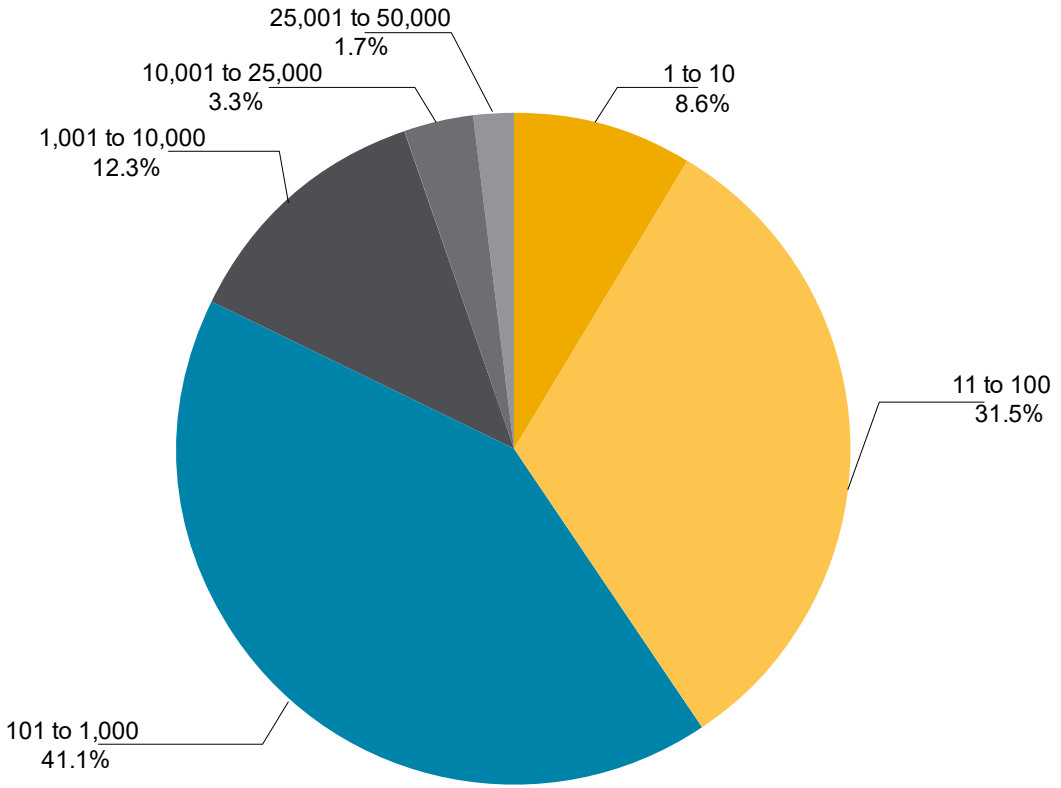
- **Key Observations:**
- Ransomware activity has dramatically **outpaced Data Breach/Privacy Event activity**.
- **Ransomware up 323%** from Q1 2019 to Q4 2021.
- Eight figure losses are commonplace – **business interruption represents the largest component of loss, litigation still to come**.
- Data exfiltration occurred in 83% of ransomware cases per Coveware in Q3 2021.
- Average days of business interruption in Q3 2021 was **22 days** per Coveware

Source: Risk Based Security, analysis by Aon. Data as of 1/31/2021; Ransomware data exfiltration and downtime per Coveware Quarterly Ransomware Report as of 10/21/2021

Ransomware Attacks by Size of Company

- Companies with 1,000 or less employees represent 81% of attacks
- Why? Mid-market, SMB companies typically have lower cyber security maturity
- Large enterprise are not immune – supply chain attacks like SolarWinds, Microsoft Exchange, JBS

Distribution by company size (Employee Count)

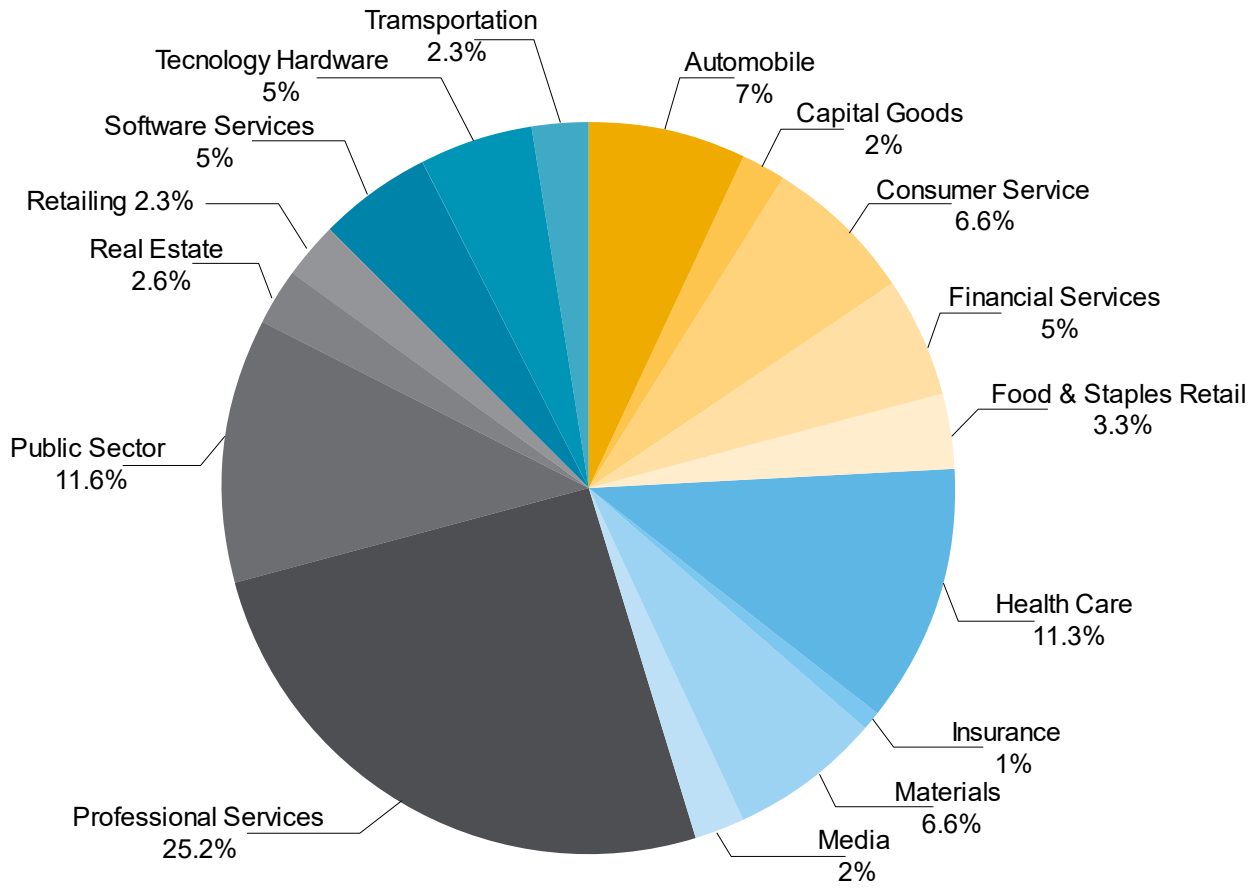


*Coveware blog, Q3 2020

Ransomware Attacks are Focused on Mid-Market and SMB

- All industries are being targeted
- Attackers are not necessarily focused on industries with PII/PHI

Common Industries Targeted by Ransomware in Q2 2021



*Coveware blog, Q3 2020

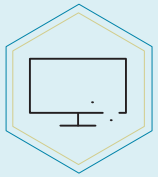
Ransomware Attacks – How Do They Happen?

The three most common attack paths for ransomware

Phishing Email

Attackers will send phishing emails to gain access with legitimate credentials and/or deploy weaponized attachments

Remote Access



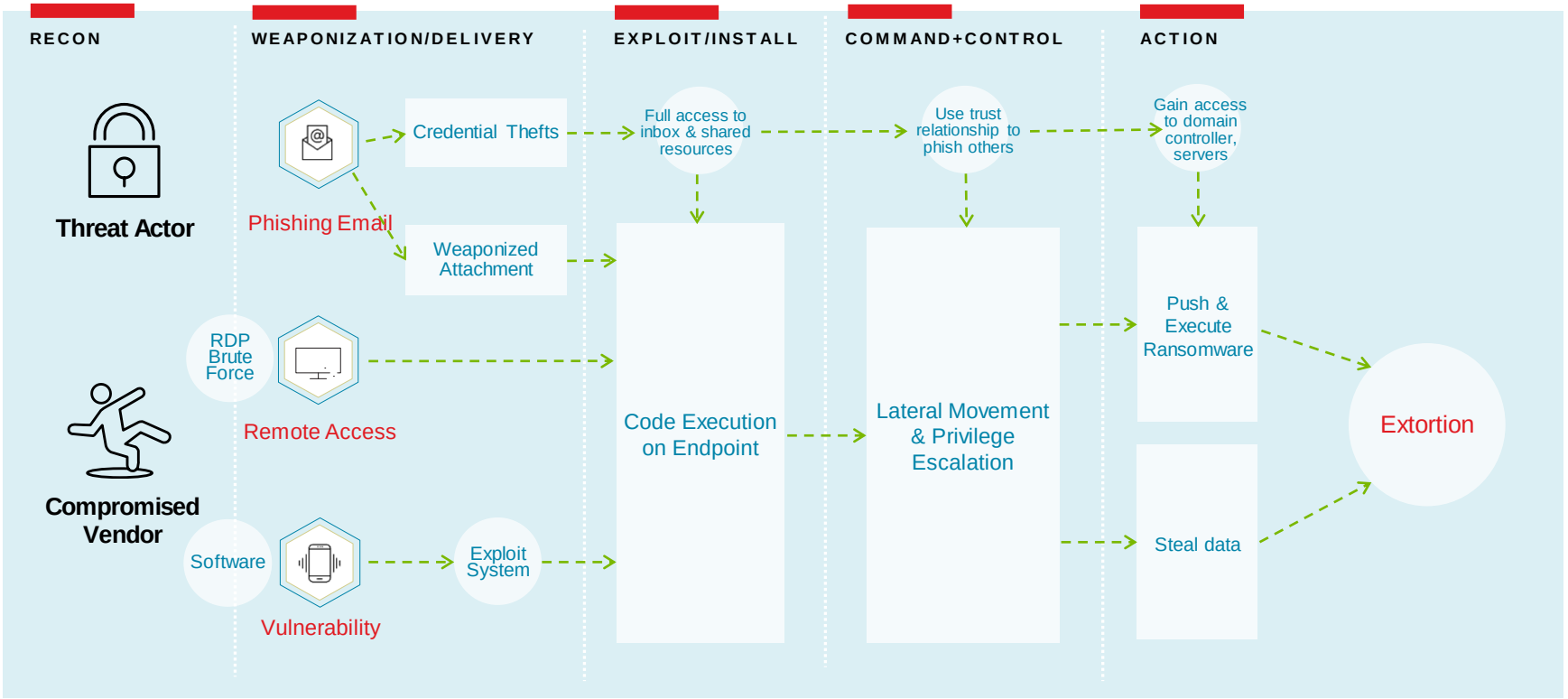
Companies use remote access technology in an insecure way that enables threat actors to gain access to their environments

Vulnerabilities

Attackers will find vulnerable perimeter devices (unpatched servers and software) and exploit them to gain access to networks

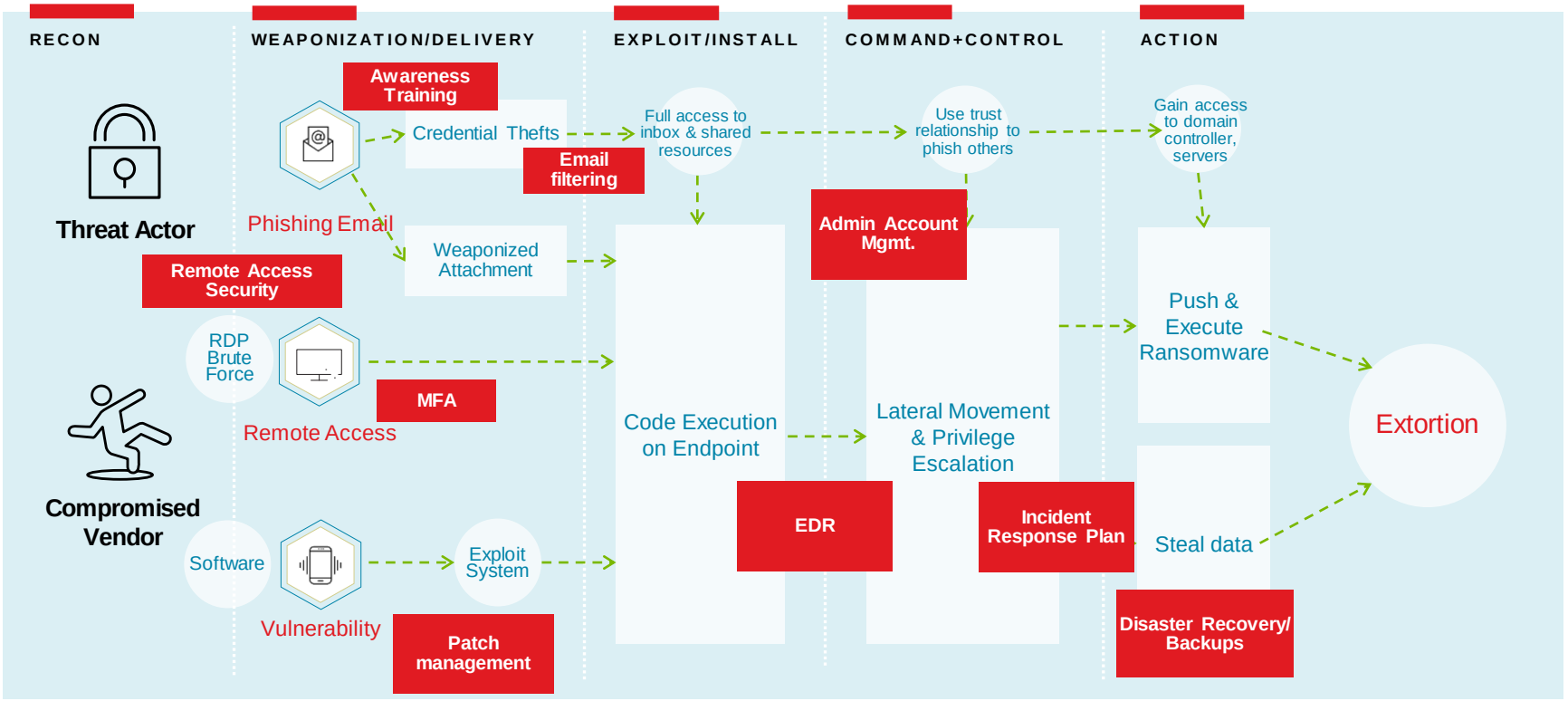
Ransomware Attacks – How Do They Happen?

From the three attack vectors, attackers deploy malware, propagate and infect other systems



Ransomware Defense – Nine Key Security Controls

A layered approach to ransomware security



Current Cyber Insurance Market

Cyber Insurance Market – Trends as of Q1 2022

Claims & Losses

- Increased frequency and severity in ransomware losses through 2020 and 2021 have caused some cyber insurer loss ratios to increase beyond sustainable levels for the product. This leads to insurers exiting the marketplace.
- Complex Cyber & Tech E&O losses have also continued to develop, with multiple severity cases in 2021 already compounding on large events that occurred over the past five years. (Kaseya, SolarWinds, Microsoft, Accellion and Log4j)
- The regulatory environment continues to gain complexity with the continuous enforcement of existing and emerging privacy legislation.

Coverage

- Insurers are hyper-focused on underwriting to ransomware controls. If controls are deemed to be insufficient or not present, ransomware related coverage will not be offered, will be sub-limited, or will be subject to co-insurance.
- Insurers continue to emphasize the use of cyber incident response panel arrangements, including use of the following pre-arranged vendors: forensics, incident response, and legal support.
- Some insurers are requiring increased waiting periods for Business Interruption/Systems Failure and adding co-insurance provisions or sub-limiting coverage for Dependent Business Interruption/Systems Failure.
- Market rumblings continue to develop around restricting coverage related to infrastructure and systemic risk arising from correlated events.

Capacity

- Insurers are actively managing their global aggregate capacity on individual programs and looking to reduce limits offered on placements that fall outside of their underwriting guidelines due to the following: class of business, attachment point, control requirements, or rate requirements.
- A limited number of insurers re exiting the space due to loss history.
- New capacity is entering the market in the form of Insurtech MGAs for the SME/& Middle Market segments.

Rate Environment

- The market conditions for Cyber & Tech E&O continued to harden in 2021 due to ransomware activity, and concerns around systemic loss aggregation events.
- Insurer feedback suggests a need for significant rate increases for all classes of business throughout the 1H 2022. Certain classes of business or client size segments may see additional rate requirements based on loss trends.
- Aon anticipates amplified rate pressure through 1H 2022. Insurers are also looking to increase retentions and may limit coverage along with the above noted rate requirements on certain placements.
- The market is maintaining rate pressure on excess placements and pushing increases on increased limit factors (ILF) to a minimum of 80-85%.

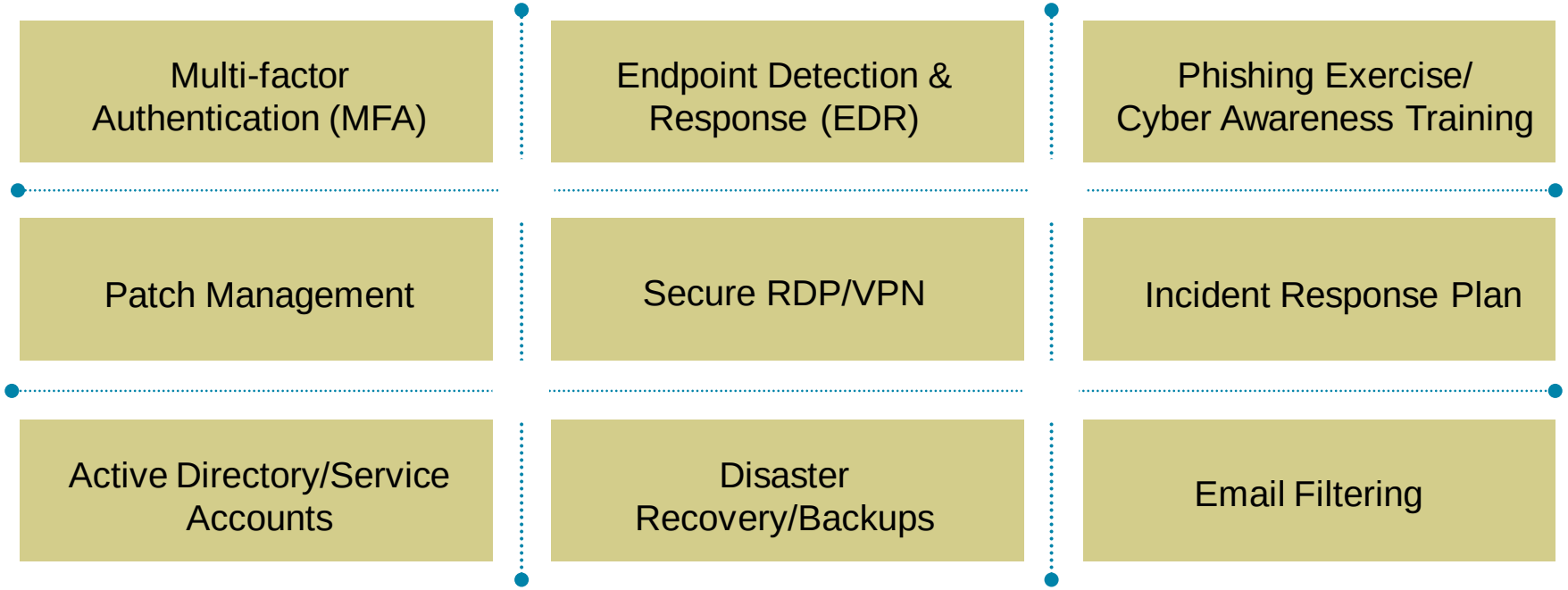
Process

- Given recent losses, insurers are looking for much more underwriting information for all risks. If there have been recent losses insures will require an overview of the loss, what steps were taken to remediate the event, what steps are being taken to mitigate this from occurring in the future, and the potential/total cost of the loss
- Many insurers are requiring an underwriting meeting in addition to a written submission; sometimes requiring their own supplemental applications. There is limited flexibility around quoting without information.
- The underwriting process is much more intensive as carriers are looking for more information. Quotes take much more time as they must reach a higher level of authority in order to quote.

Cyber Underwriting Focus

Nine Cyber Security Control Areas that Underwriters Care About

- Ransomware Supplemental Addendum started January 2021 in addition to the standard Cyber form
- More technically detailed questions
- Rigorous underwriting
- Insureds need to have positive responses for ALL key areas of focus



Common Insurer Reasons for Declination

Multi-Factor Authentication (MFA)

- Lack of universal use of MFA for remote access and monitoring hours
- MFA is not implemented across the board for privileged access
- MFA not in place for backups or Remote Desktop Protocol

Endpoint Detection & Response (EDR)

- Lack of EDR Solution in place
- EDR is not tuned to be in “Block Mode”
- EDR is not deployed across more than 90% of the environment

Patch Management

- Despite their infrastructure begin hosted on their behalf, we need to see policies in place for patch management as well as Business Continuity
- Lack of a Patch Management policy for tracking and deploying critical or “out-of-band” patches

Active Directory / Service Accounts

- We have concerns surrounding admin rights (separate credentials, use of MFA)
- Too many service accounts for the number of applications
- No Active Directory in place

Incident Response Plan / Phishing Awareness

- No dedicated plan for Ransomware Response
- Lack of internal Phishing Awareness Training

Appendix

Aon's Cyber Solutions and the Stroz Friedberg Incident Response Team

are world-class cyber security professionals building confidence in a world of uncertainty. Offering holistic cyber risk management solutions, unsurpassed investigative skills, and proprietary technologies, we help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

Our clients call us — and we're at our best — when **the stakes are high and the potential for damage is great**. We are united by a common goal: **to protect today and safeguard tomorrow**.

Find out more at **aon.com/cyber-solutions**.

We're standing by.

Our Solutions

Your **MSA/Retainer** gives you streamlined access to the entire breadth of Aon's Cyber Solutions / Stroz Friedberg capabilities. Contact **Stefan Toi** to learn more.

Stroz Friedberg Digital Forensics & Incident Response

Helping to solve your cyber events

Respond to the incident, create an investigation strategy, and help contain the incident while preserving evidence and confidently communicating with your stakeholders, helping you get your business back to operational status as quickly and as safely as possible.

Investigations

Uncovering the facts

Combine advanced analytics and investigative capabilities to perform complex financial investigations, forensic accounting, and compliance assessments.

eDiscovery

Navigating the complex issues

Analyze evidence to target, understand, and present the key findings in a reasonable, efficient, and defensible manner.

Intelligence

Intelligence can create strategic advantage

Conduct proactive and reactive threat monitoring and provide tailored intelligence reports and analysis to help mitigate vulnerabilities.

Security Advisory

Assessing, managing and mitigating cyber risk

Evaluate and help remediate your vulnerabilities, determine your readiness to respond, and improve your organization's cyber resilience.

Security Testing

Identifying your systems' vulnerabilities

Leverage real-world testing and simulations to help you better understand your weaknesses and strengthen your defenses.

Cutting Edge Security Research:
https://aon.io/CyberLabs

Quantification

Optimizing your total cost of risk

Model cyber loss scenarios to stress test your current cyber insurance strategy and prioritize security investments.

Cyber Quotient Evaluation (CyQu)

Rapidly size up your cyber risk through self-assessment

Rapidly evaluate your enterprise cyber security posture to help develop a data-driven cyber risk management strategy.

AON
Empower Results®

Holistic risk mitigation strategies and solutions.

Seek

We help you understand and quantify your risk.

- Assessments
  - > Security Risk Assessment
  - > CyQu
  - > Cyber Impact Analysis: Financial Quantification
  - > Incident Response Readiness Assessment
  - > Compromise Assessment
  - > Security Architecture Assessment
  - > Privacy Compliance Assessment
  - > Insider Risk Assessment
  - > Executive Vulnerability Assessment
- Testing
  - > Red Team & Social Engineering Testing
  - > Application & Mobile Security Testing
  - > Network & Cloud Penetration Testing
  - > Cloud & Host Configuration Review
  - > Automotive & IoT Security Testing
  - > Source Code Security Review
- Due Diligence & Background Investigations

Shield

We know how to protect your organization and its critical assets.

- Cyber Insurance
- Cyber Risk Financing
- Incident Response Planning & Playbook Development
- Cyber Threat Simulation/Tabletop
- Security Architecture & Design
- Security Policies & Standards Development
- Security Strategy Development
- Security Controls Optimization
- Third Party Cyber Risk Management
- Insider Risk Program Development
- M&A Cyber Due Diligence
- Secure Software Development Lifecycle
- SOC Optimization
- CISO Advisory
- Board Advisory
- Fraud Prevention

Solve

We search for the truth and help you recover quickly.

- Stroz Friedberg Incident Response
- Stroz Friedberg Digital Forensics
- eDiscovery
- Expert Witness Testimony
- Incident Response Retainer
- Complex Cyber Loss Preparation
- Claims Advocacy
- Fraud & Financial Loss Investigations
- Workplace Misconduct Investigations

Thank You!

Stefan R. Toi
Vice President
Stroz Friedberg, an Aon Company
+1.646.275.2419
Stefan.toi@aon.com

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management solutions, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

aon.com/cyber-solutions