resilience

Cyber Risks and Mitigation Strategies

RIMS - Central Texas Chapter

April 20, 2023

Presenters

Michael Manzo

Vice President - Underwriting

michaelmanzo@cyberresilience.com

+1 214.537.1336

Kevin Neslage

US Incident Response
Claims Counsel

kevinneslage@cyberresilience.com

+1 305.934.9986

resilience

Evolution of the Cyber Market

Evolution of Cyber Attacks

- 1980’s - 90’s - Cyber Crime is born - Stealing Valuable information for profit
- Target industries were banks, retailers, hospitals
- 2010 - current - Data loses value and Ransomware Rises
- All industries are targeted - sectors that were not required to invest in cyber security were hit especially hard.

Cyber Coverages

- **Breach response coverages:** costs may include those incurred to hire breach counsel, complete a forensic investigation, hire a public relations firm, notifications to affected individuals, call center services, ID theft restoration/credit monitoring.

- **Network security & privacy liability coverage:** coverage for indemnity and defense costs for third-party claims and regulatory actions alleging a security failure or privacy event.

- **Regulatory Fines & Penalties:** monetary fines and penalties an insured is legally obligated to pay due to a regulatory proceeding by a governmental entity.

- **Media liability**: Coverage for indemnity and defense costs for third-party claims alleging media wrongful acts, such as defamation, disparagement and copyright/trademark infringement in the dissemination of internet content and media

- **Business interruption/System Failure:** Indemnification for loss of income, incurred extra expenses and claims preparation costs that arise directly out of a network outage due to an unplanned outage

- **Dependent business interruption/System Failure:** Extends the business interruption to cover your lost income and extra expenses incurred due to a network interruption, occurring at one of your critical third parties or outsourced providers that you rely on to conduct business.

- **Data Recovery:** Costs to rebuild, restore, replace electronic data or software corrupted or deleted in a cyber event

- **Cyber extortion/ransomware:** Covers extortion payments and associated expenses to investigate a security threat to release or refuse to unencrypt sensitive information or to bring down a network unless a ransom is paid.

- **Cyber Crime:** May include direct financial loss due to Telephone Fraud, Cryptojacking, Social Engineering, Invoice Manipulation, Transfer Fraud.

- **Reputational Harm:** loss of net profit an insured would have earned if not for an adverse media event

- **Computer Hardware Replacement costs (Bricking):** replacement costs for computer hardware and devices or equipment left unusable due to a cyber event

The Resilience Policy

COST

Emergency Coverages
for your incident response.

Response

Data Recovery

Hardware Replacement

LOSS

First-Party Coverages
to help you recover.

Interruption Loss

Extortion

Social Engineering

Invoice Manipulation

LIABILITY

Third-Party Coverages
to defend you.

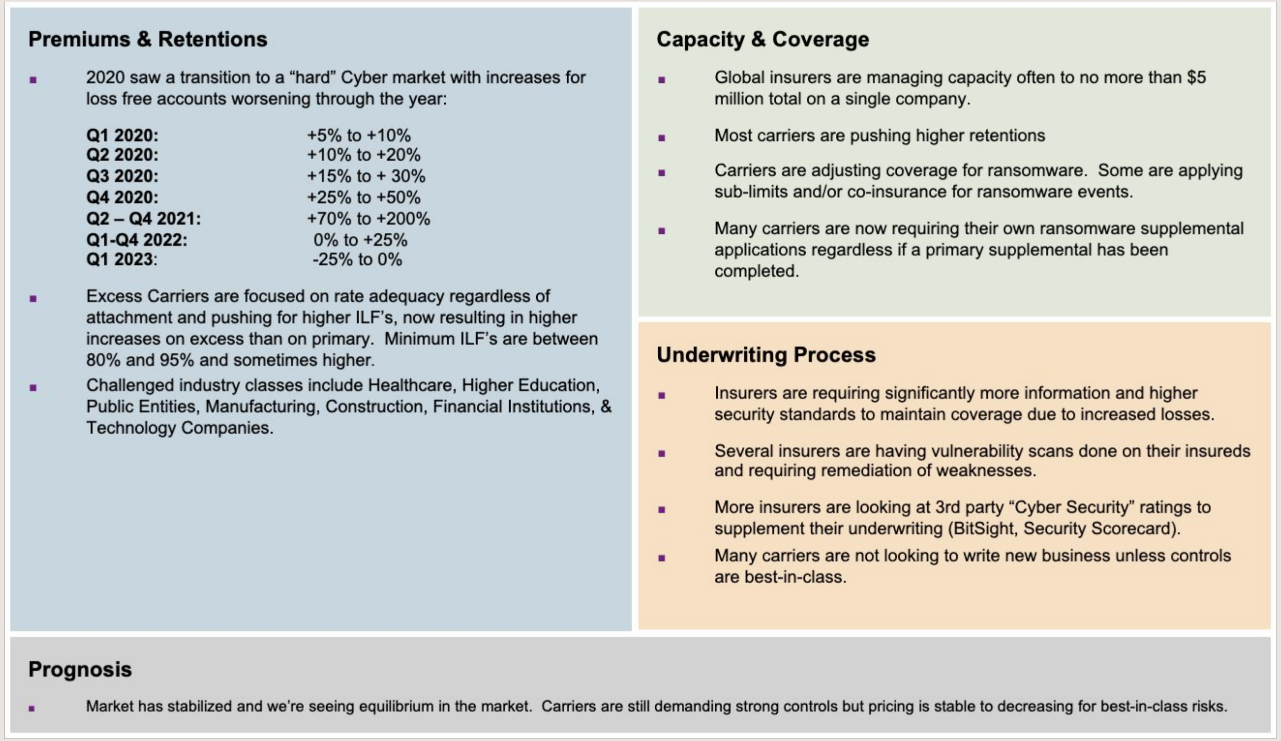
Data & Network

Regulatory

resilience

Underwriting and Claims Trends

Cyber Market Update - Q1 2023



Premiums & Retentions

- 2020 saw a transition to a "hard" Cyber market with increases for loss free accounts worsening through the year:

Q1 2020:	+5% to +10%
Q2 2020:	+10% to +20%
Q3 2020:	+15% to + 30%
Q4 2020:	+25% to +50%
Q2 – Q4 2021:	+70% to +200%
Q1-Q4 2022:	0% to +25%
Q1 2023:	-25% to 0%

- Excess Carriers are focused on rate adequacy regardless of attachment and pushing for higher ILF's, now resulting in higher increases on excess than on primary. Minimum ILF's are between 80% and 95% and sometimes higher.
- Challenged industry classes include Healthcare, Higher Education, Public Entities, Manufacturing, Construction, Financial Institutions, & Technology Companies.

Capacity & Coverage

- Global insurers are managing capacity often to no more than $5 million total on a single company.
- Most carriers are pushing higher retentions
- Carriers are adjusting coverage for ransomware. Some are applying sub-limits and/or co-insurance for ransomware events.
- Many carriers are now requiring their own ransomware supplemental applications regardless if a primary supplemental has been completed.

Underwriting Process

- Insurers are requiring significantly more information and higher security standards to maintain coverage due to increased losses.
- Several insurers are having vulnerability scans done on their insureds and requiring remediation of weaknesses.
- More insurers are looking at 3rd party "Cyber Security" ratings to supplement their underwriting (BitSight, Security Scorecard).
- Many carriers are not looking to write new business unless controls are best-in-class.

Prognosis

- Market has stabilized and we're seeing equilibrium in the market. Carriers are still demanding strong controls but pricing is stable to decreasing for best-in-class risks.

Key Areas of Underwriting Focus

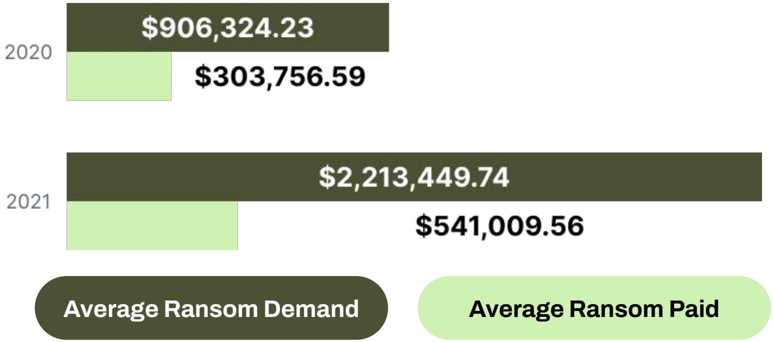
- Multi-factor Authentication (remote access, Cloud Resources, email, Admin/Priv Accounts)
- Open RDP Ports
- Backups (offline, encrypted, segmented, how often are they tested?)
- Employee Training / Phishing Awareness
- E-mail Filtering
- Patching cadence (response time, patching success)
- Endpoint Security (tools implemented, what percentage of the organization, is there an incident response team)
- Unprotected End of Life Exposures
- IT / OT Segmentation

Threats & Trends

Top Threats

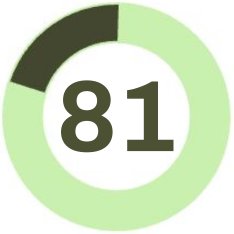
- **Ransomware & Business Email Compromise**
- **Most Common Attack Vectors** - Phishing Emails & Poorly Secured RDP
- **Significant Drivers of Loss**
  - Business Interruption Loss
  - Data Recovery Cost
  - Privacy Exposures
  - The Ransom
- **Most Common Threat Actors**
  - Lockbit
  - Conti
  - Aveddon
  - Ryuk
  - REvil

Ransomware Business Impacts



23

Days of Average Downtime*



Percent of attacks that threat to expose of stolen data*

Third-Party Litigation

Data Breach Liability

- Litigation that typically arises out of a data breach
- Most policies include coverage for regulatory liability

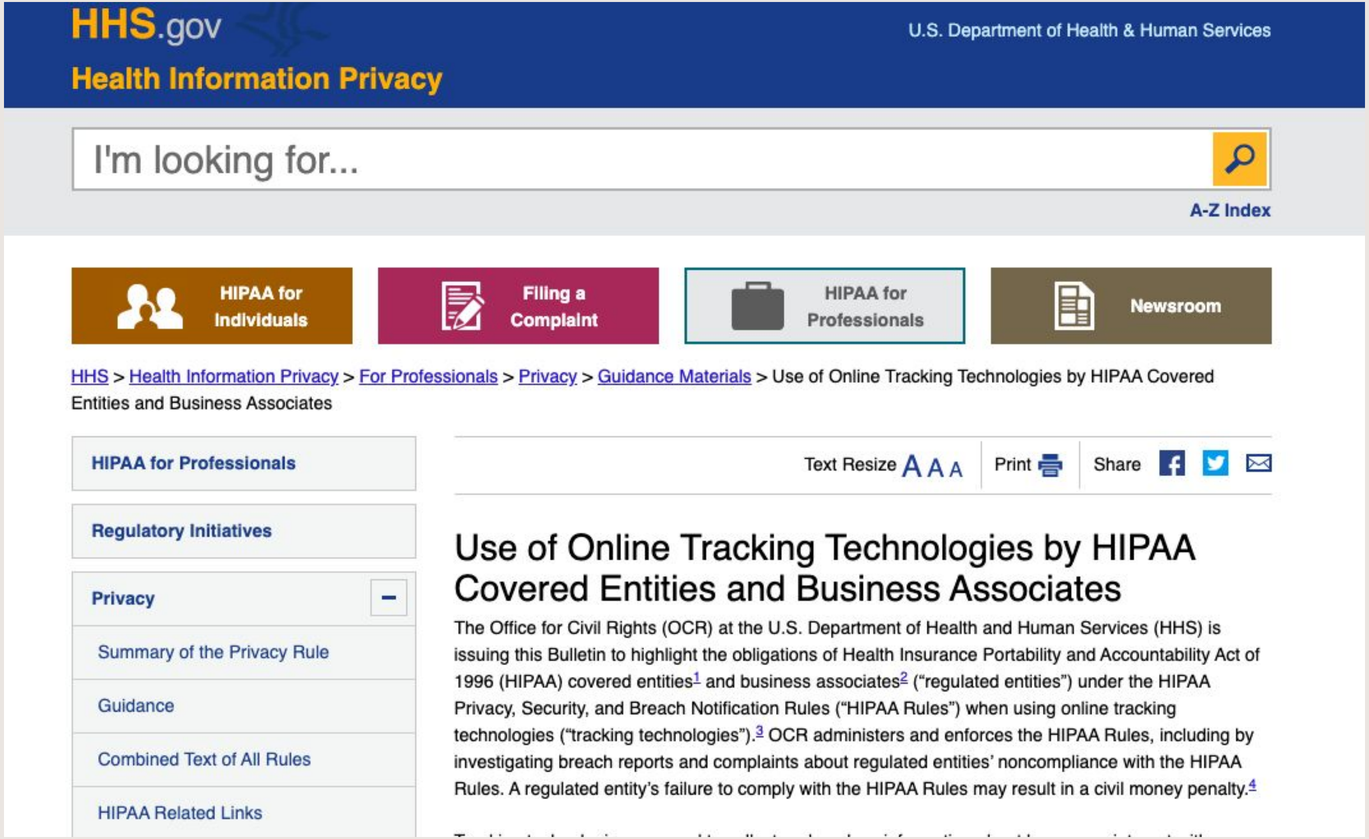
Web Tracking Liability

- Litigation arising from collection of information on an insured's website
- Drastic increase in class action litigation in 2023 across the country, mostly in the healthcare sector

Media Liability

- Arises from violating another parties' intellectual property rights
- Often related to information published on website

Liability arising from use of Facebook’s Pixel



HHS > Health Information Privacy > For Professionals > Privacy > Guidance Materials > Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) is issuing this Bulletin to highlight the obligations of Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities[1] and business associates[2] (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technologies (“tracking technologies”).[3] OCR administers and enforces the HIPAA Rules, including by investigating breach reports and complaints about regulated entities’ noncompliance with the HIPAA Rules. A regulated entity’s failure to comply with the HIPAA Rules may result in a civil money penalty.[4]

Continued Increase in Privacy Legislation

TITLE

State Level

- Comprehensive Privacy Legislation
  - Texas HB 1844
- Biometric Privacy Laws
- State Judicial Decisions

TITLE

US Federal Level

- ADPPA bill
- Increased Regulatory Action (HHS, FTC, FDA)
- Federal Judicial Decisions

TITLE

International Level

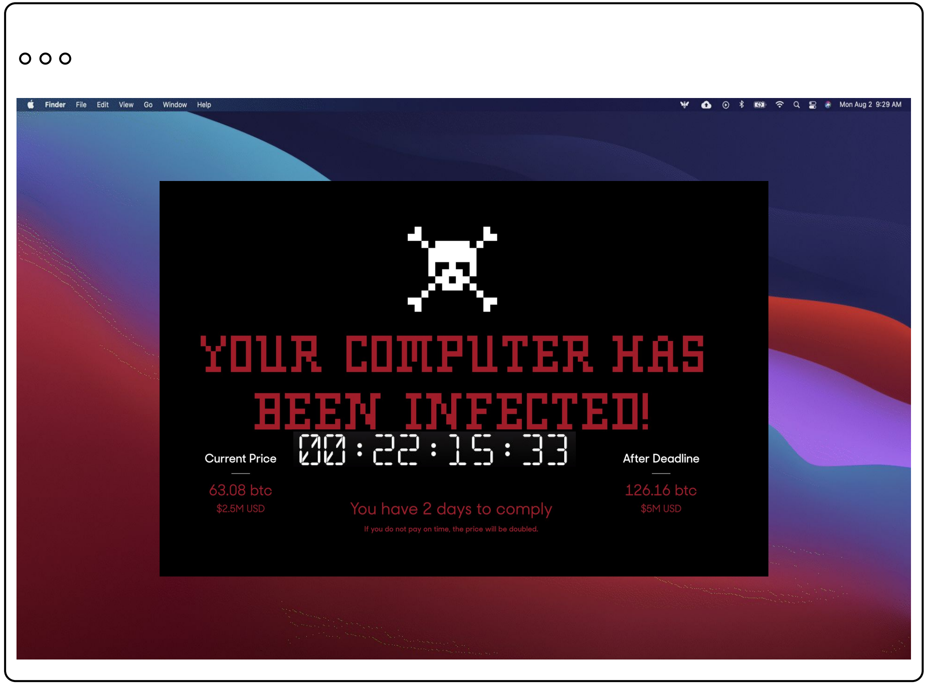
- European GDPR
- Canadian, UK Privacy Reform
- Worldwide legislations being enacted

resilience

Incident Response

Setting the Scene

- Employees are unable to access files on their workstations.
- IT begins to receive a flood of calls from frustrated employees - quickly discovering data on their servers is encrypted.
- A ransom note demands $2.5MM in exchange for a decryption key. The price will double in 24 hours if they don't hear from you.



YOUR COMPUTER HAS BEEN INFECTED!

00:22:15:33

Current Price

63.08 btc

$2.5M USD

After Deadline

126.16 btc

$5M USD

You have 2 days to comply

If you do not pay on time, the price will be doubled.

Responding to Ransomware

- Follow CISA’s Ransomware Response Checklist as a guide.
- Activate your incident response plan.
- Isolate impacted computers immediately.
- Secure your backup data and systems.
- Report to law enforcement.
- Engage expertise.

The Situation Develops

- Email and other business-critical systems are down. Construction sites are brought to a halt; payroll is disrupted.
- Word of the cyber attack spreads. Business partners are asking for a resolution, and a journalist reached out for a comment on the data breach.
- IT Department confirms that backups are encrypted.
- Threat actor claims to have stolen 100GB of data, including private information about employees, customers, and business operations.

Incident Response & Containment

Legal

Forensics

Crisis Management

Business Continuity

Ransom Resolution

Data Recovery

Data Breach?

Notification

Call Center

Credit Monitoring

To Pay or Not To Pay?

Data Encryption

- Are all viable backups encrypted and have we tested their ability to recover?
- Are there any other means of rebuilding or restoring computer systems?
- Can we endure how long it will take to rebuild vs paying the demand?
- Can we trust that the decryption key will work to recover our data?

Data Exfiltration

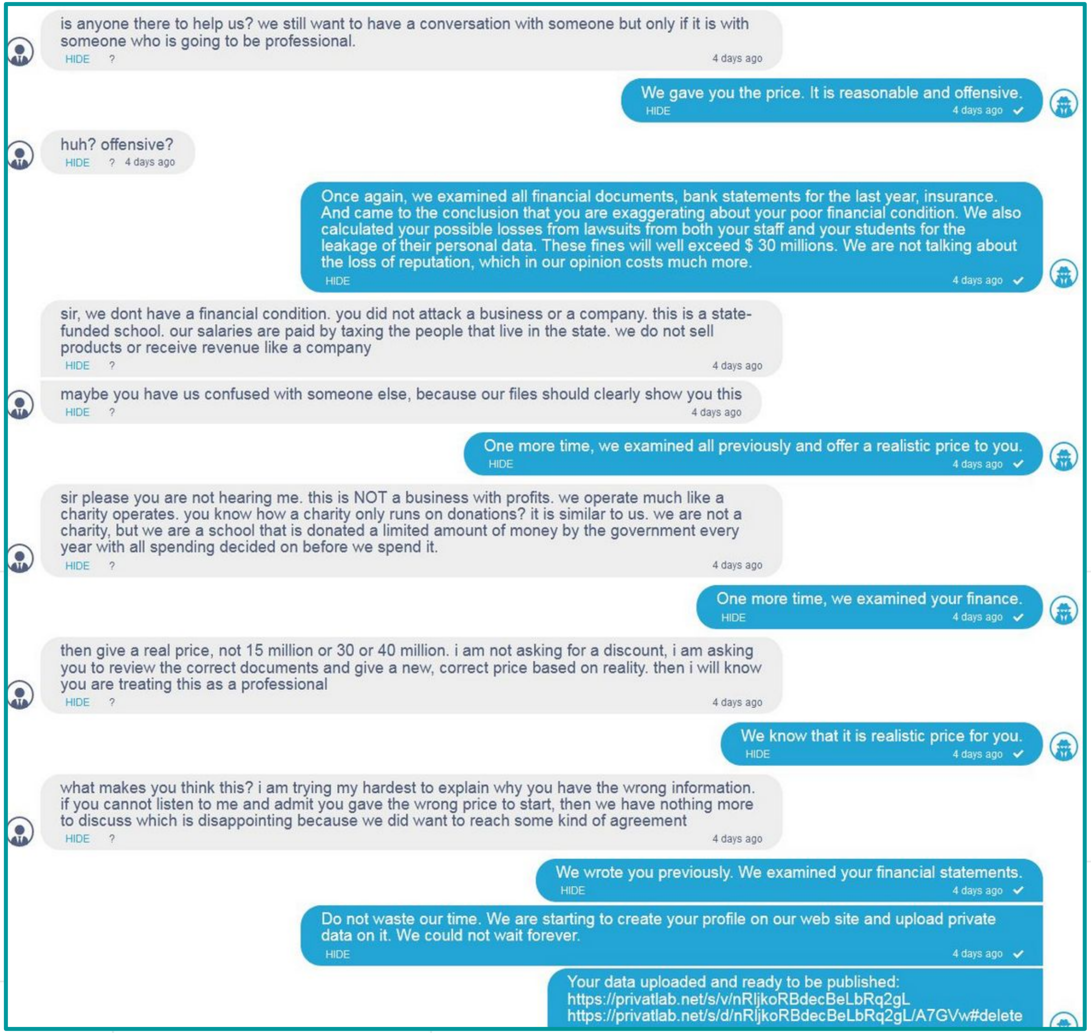
- What data was stolen and how do we know?
- What are the legal and reputational ramifications if the data is leaked?
- Does making the payment reduce potential risk to clients and employees?
- Do we still have data breach notification obligations to clients and/or employees?

Payment Logistics

- Who within the organization has the authority to authorize a potential payment?
- Is it legal to make the payment?
- Do we have access to enough funds to make the payment?
- How will we obtain the Bitcoin and make the payment to the threat actor?

Conti

Ransom Negotiations



is anyone there to help us? we still want to have a conversation with someone but only if it is with someone who is going to be professional.
HIDE ? 4 days ago

We gave you the price. It is reasonable and offensive.
HIDE 4 days ago ✓

huh? offensive?
HIDE ? 4 days ago

Once again, we examined all financial documents, bank statements for the last year, insurance. And came to the conclusion that you are exaggerating about your poor financial condition. We also calculated your possible losses from lawsuits from both your staff and your students for the leakage of their personal data. These fines will well exceed $ 30 millions. We are not talking about the loss of reputation, which in our opinion costs much more.
HIDE 4 days ago ✓

sir, we dont have a financial condition. you did not attack a business or a company. this is a state-funded school. our salaries are paid by taxing the people that live in the state. we do not sell products or receive revenue like a company
HIDE ? 4 days ago

maybe you have us confused with someone else, because our files should clearly show you this
HIDE ? 4 days ago

One more time, we examined all previously and offer a realistic price to you.
HIDE 4 days ago ✓

sir please you are not hearing me. this is NOT a business with profits. we operate much like a charity operates. you know how a charity only runs on donations? it is similar to us. we are not a charity, but we are a school that is donated a limited amount of money by the government every year with all spending decided on before we spend it.
HIDE ? 4 days ago

One more time, we examined your finance.
HIDE 4 days ago ✓

then give a real price, not 15 million or 30 or 40 million. i am not asking for a discount, i am asking you to review the correct documents and give a new, correct price based on reality. then i will know you are treating this as a professional
HIDE ? 4 days ago

We know that it is realistic price for you.
HIDE 4 days ago ✓

what makes you think this? i am trying my hardest to explain why you have the wrong information. if you cannot listen to me and admit you gave the wrong price to start, then we have nothing more to discuss which is disappointing because we did want to reach some kind of agreement
HIDE ? 4 days ago

We wrote you previously. We examined your financial statements.
HIDE 4 days ago ✓

Do not waste our time. We are starting to create your profile on our web site and upload private data on it. We could not wait forever.
HIDE 4 days ago ✓

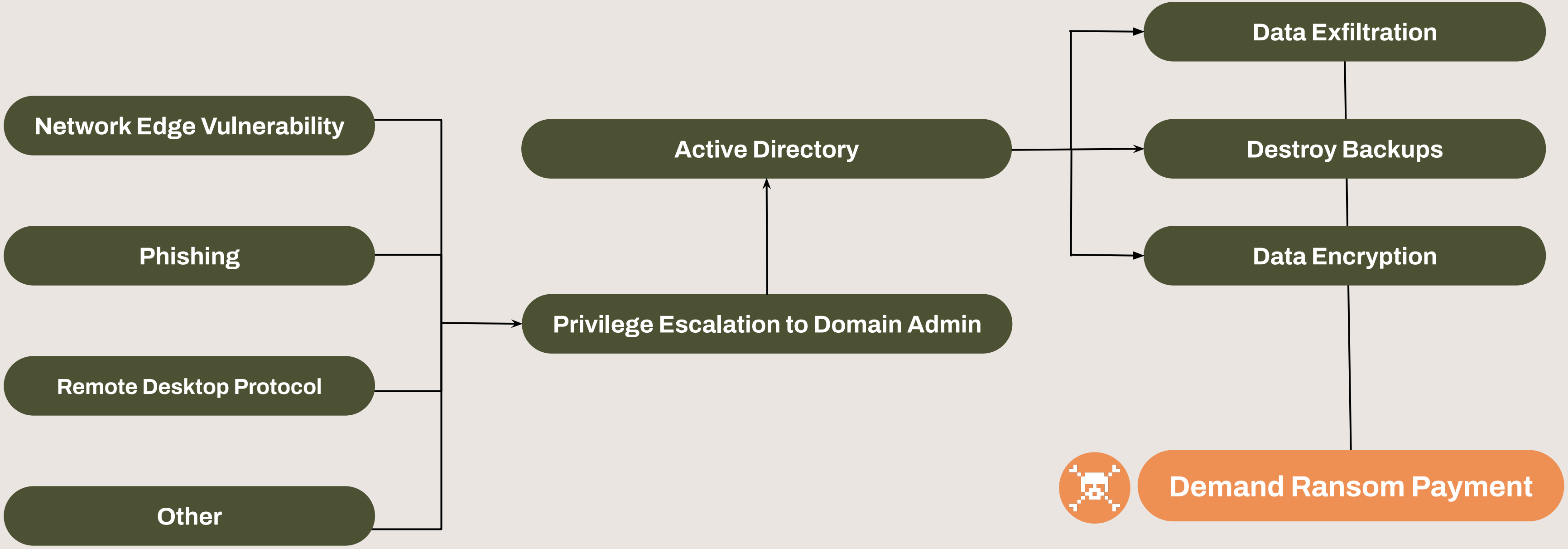
Your data uploaded and ready to be published:
https://privatlab.net/s/v/nRljkoRBdecBeLbRq2gL
https://privatlab.net/s/d/nRljkoRBdecBeLbRq2gL/A7GVw#delete

resilience

Cyber Resilience

What happened?

It begins... Initial Compromise



Network Edge Vulnerability

Phishing

Remote Desktop Protocol

Other

Privilege Escalation to Domain Admin

Active Directory

Data Exfiltration

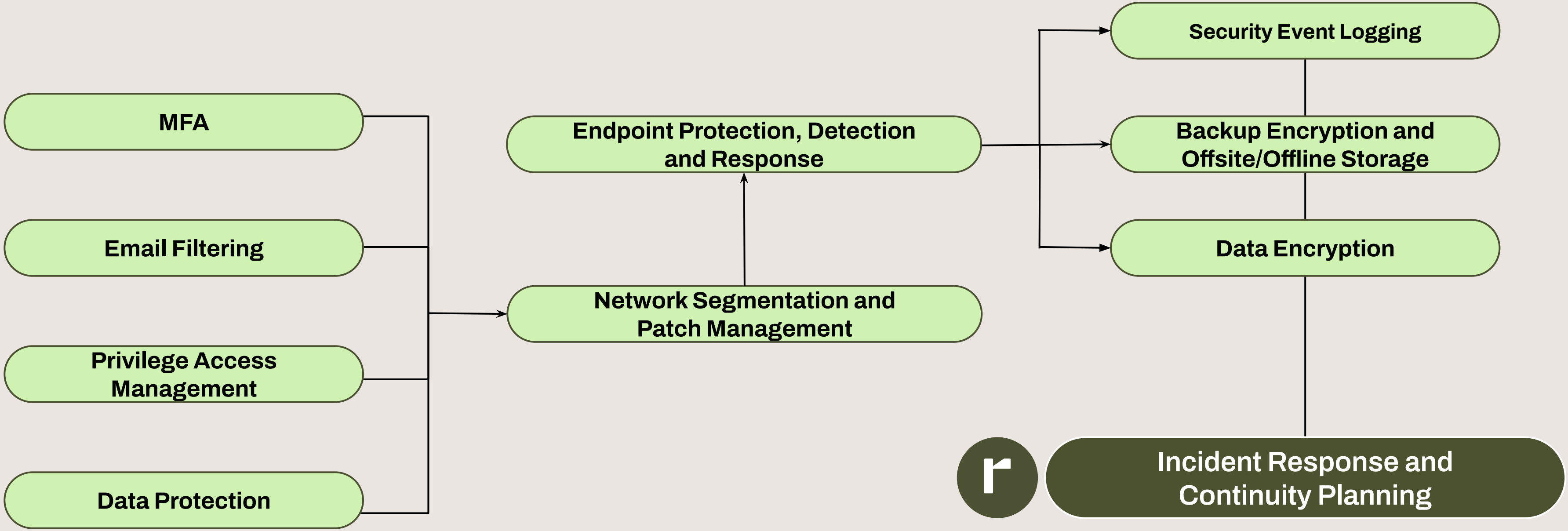
Destroy Backups

Data Encryption

Demand Ransom Payment

Mitigation Controls

Preventing Initial Compromise


MFA
Email Filtering
Privilege Access Management
Data Protection
Network Segmentation and Patch Management
Endpoint Protection, Detection and Response
Security Event Logging
Backup Encryption and Offsite/Offline Storage
Data Encryption
Incident Response and Continuity Planning

What steps can everyone take today?

- Don’t click on links in spam, unexpected or suspicious emails.
- Ensure that your security software and operating system are up to date.
- Use multi-factor authentication on your important online accounts.
- Regularly back up data stored on your computer, so a ransomware infection wouldn’t destroy your most important data forever.

What is the Cyber Primary Care Program?

For us, your risk is our risk, and Cyber Primary Care is the program that we have developed as an annual engagement that augments your cybersecurity resources - people, expertise, and capital - to effectively and holistically manage their risk and become Cyber Resilient.

PRODUCT

Access to the Resilience Cyber Primary Care portal.

Bi-weekly external scans and security threat updates.

PEOPLE

Security focused cadence calls.

Trusted resources for guidance and a network of partners.

PROCESS

Manage controls with tools to reduce the organizations attack surface.

Track exposures on the dark web, establish or improve a cyber security governance program.

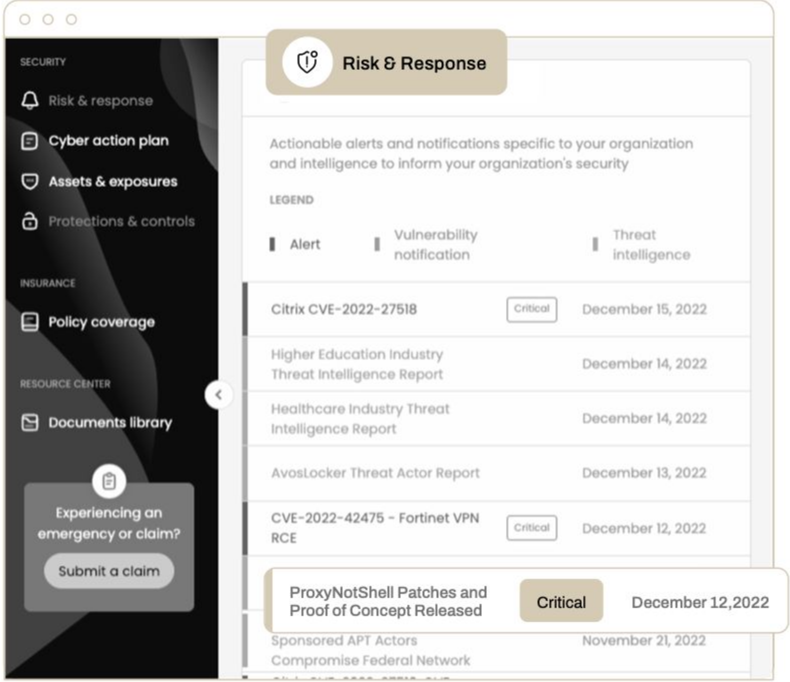
Resilience Approach: Cyber Primary Care Program Outcomes

- Cyber Primary Care program helped fast-track remediation.
  - Critical external misconfigurations & exposures to reach **100% remediation rate.**
  - Critical WEB (HTTP/HTTPS) vulnerabilities to reach a 100% remediation rate.

- Provided recommendations that increased the organization's **cybersecurity budget by 4X.**

- Helped the client access **50X the coverage** for the same premium on ransomware.

- Improved insurability despite cyber events and losses.



Actionable alerts and notifications specific to your organization and intelligence to inform your organization's security

Citrix CVE-2022-27518	Critical	December 15, 2022
Higher Education Industry Threat Intelligence Report		December 14, 2022
Healthcare Industry Threat Intelligence Report		December 14, 2022
AvosLocker Threat Actor Report		December 13, 2022
CVE-2022-42475 - Fortinet VPN RCE	Critical	December 12, 2022
ProxyNotShell Patches and Proof of Concept Released	Critical	December 12,2022
Sponsored APT Actors Compromise Federal Network		November 21, 2022

Questions?