EPIC®
Insurance Brokers & Consultants

bms.

Cyber Insurance Overview

FACT Risk Management Conference

©2024 Edgewood Partners Insurance Center. All rights reserved. | CA License: 0B29370

Agenda

Overview a Cyber Policy

- Coverages and Examples

Cyber Market Cycle and Trends

- What has happened over time

Social Engineering and Ransomware

- Why it became an Epidemic, where has it gone?
- Florida's No Ransomware Payments Legislation

Key Cyber Security Controls

- With some awful examples! Sorry!

Cyber

Who is Covered?

Most of the coverage is tied to the network.

Cyber policies cover the named insured and any subsidiary at the time the policy is placed.

In addition, insureds under the policy include senior executives and employees. It is also common to see independent contractors included in the definition of insured.

Cyber Policy

What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

01 Security Failure or System Failure

02 External or Internal Threat Actor

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

Breach Response Costs

01 Crisis Management

02 IT Forensics

03 Public Relations

04 Legal Advice

05 Notification Expenses

Crime

01 Fraudulent Instruction

02 Funds Transfer Fraud

03 Telephone Fraud

04 Invoice Manipulation

05 Cryptojacking

Cyber

What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

Cyber
What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

MORRISONS

aetna℠

Cyber

What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

Cyber

What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

Cyber
What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

Breach Response Costs

01 Crisis Management

02 IT Forensics

03 Public Relations

04 Legal Advice

05 Notification Expenses

Cyber
What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

Breach Response Costs

01 Crisis Management

02 IT Forensics

03 Public Relations

04 Legal Advice

05 Notification Expenses

Cyber

What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

01 Security Failure or System Failure

02 External or Internal Threat Actor

Breach Response Costs

01 Crisis Management

02 IT Forensics

03 Public Relations

04 Legal Advice

05 Notification Expenses

Cyber

What's Covered

Third Party Liability

01 Privacy Liability

02 Network Security Liability

03 Regulatory & PCI Fines

First Party Costs

01 Data Restoration

02 Business Interruption

03 Cyber Extortion

Breach Response Costs

01 Crisis Management

02 IT Forensics

03 Public Relations

04 Legal Advice

05 Notification Expenses

Crime

01 Fraudulent Instruction

02 Funds Transfer Fraud

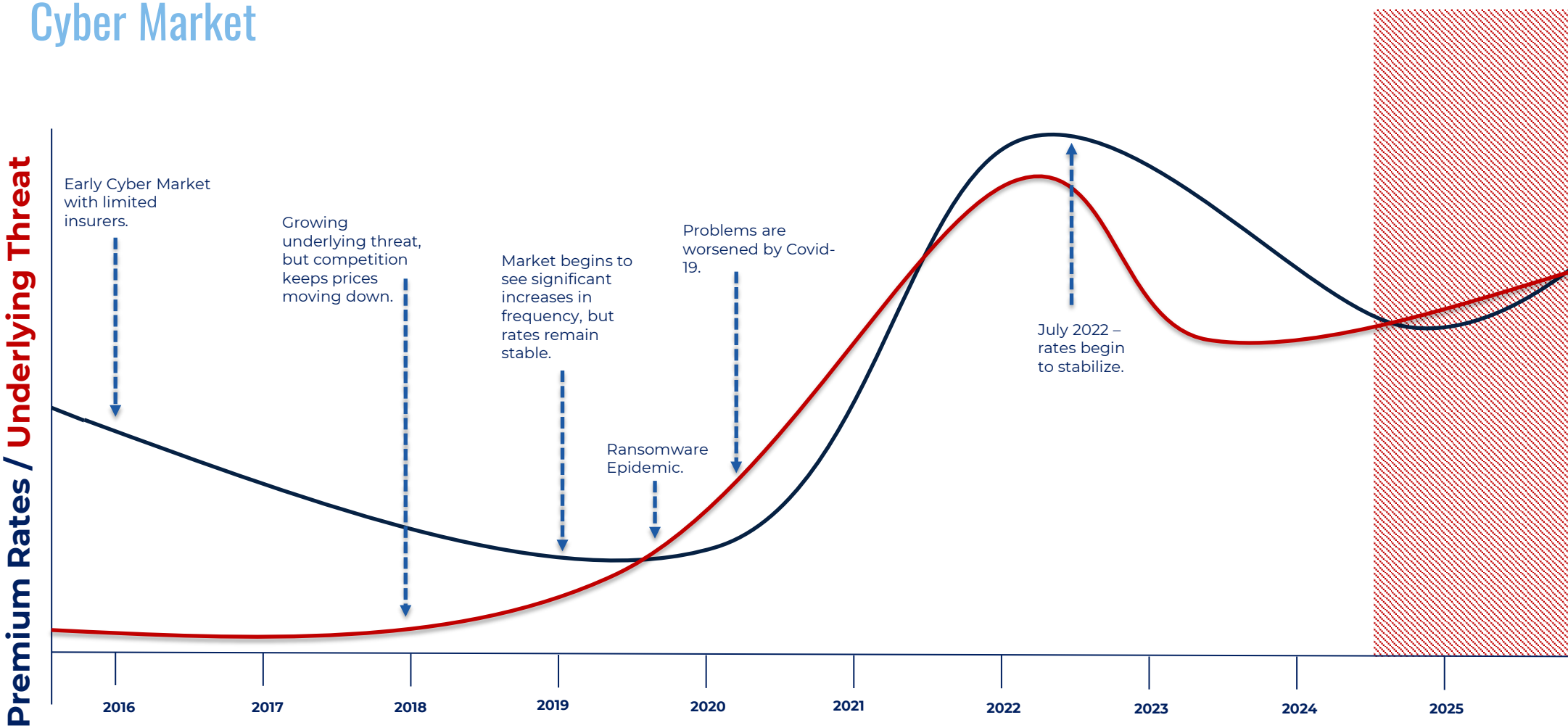
03 Telephone Fraud

01 Security Failure or System Failure

02 External or Internal Threat Actor

Market Cycles

Cyber Market



Market Update Q3 2024 – Cyber & Technology

State of the Market

- Insureds can anticipate continued flat rates with potential reductions through Q3 2024. That said, cyber attacks continue to rise, and therefore, some carriers may seek rate increases.
- Limits of $10 million on both primary and excess layers are readily accessible in the marketplace with certain carriers offering even greater capacity.
- Key controls underwriters look for remain unchanged for larger placements and include Comprehensive Multi-Factor Authentication (MFA), Network Segregation/Segmentation, Strong Data Backup Strategy, Security Awareness Training for Employees, Endpoint Detection and Response (EDR), Anti- Malware, and email security with advanced filtering.
- Insurers are beginning to ask more questions surrounding the use of Generative AI, Biometrics and Privacy Controls.

Legal & Regulatory Developments

- As a result of the Change Healthcare incident, the U.S. Department of Health and Human Services updated its site on July 30, 2024 stating under the *HITECH Act and Breach Notification Rule*, the covered entity is ultimately responsible for breach notifications. Affected covered entities should coordinate with Change Healthcare and United Healthcare Group to determine who will be providing the required breach notifications.
- Kaspersky Lab, a Russian cybersecurity company, began shutting down U.S. operations as of July 20, 2024, after the U.S. Department of Commerce announced a **ban on Kaspersky selling products in the United States**. Products must be phased out of all U.S. networks by September 29, 2024. This ban grew out of concerns for the need to protect U.S. data from foreign adversaries.
- The U.S. Senate passed legislation on Tuesday July 30, 2024 protecting children from dangerous online content. The House has not yet acted on the bill. If passed, it would provide a pathway to strengthening online privacy laws.

Emerging Risks & Trouble Spots

- On Friday, July 19, 2024, CrowdStrike informed its customers that “a defect [was] found in a single content update of its software on Microsoft Windows operating systems.” CrowdStrike’s CEO advised that the issue had been identified and was isolated. Threat actors capitalized on the incident by sending phishing emails to affected users pretending to install an update, when in fact they were installing malware onto their systems. **The CrowdStrike incident highlights the importance of vendor due diligence and management.**
- The lack of MFA for Snowflake Databases led to multiple company breaches, including breaches at Ticketmaster, AT&T, various financial institutions and others.
- There appears to be an increase in ransomware activity driven by the utilization of Generative AI along with outdated security practices such as legacy MFA systems.
- The rise of QR Code and AI-Generated phishing threats has increased interest in obtaining personal coverage. Threat actors use Generative AI to create more sophisticated phishing emails with fewer grammatical errors, making them more difficult to detect by the average person.

Social Engineering

What can be done?

Employee Training

- Phishing Simulations
- Remedial Training
- Employee Onboarding

Robust Email Controls

- DKIM/DMARC/SPF

Call Back Procedures

- Secondary Authentication
- Out-of-Band

New Exploits

- Deep Fakes
- AI
- Phishing/Smishing/Quishing

Ransomware

What is it?

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.

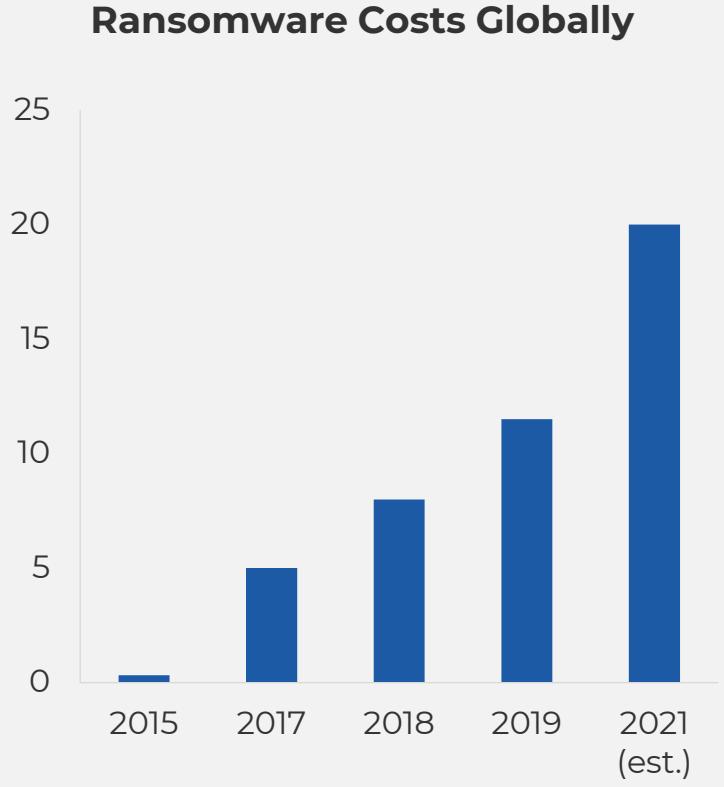
11
Ransomware attacks a second

3m
Attacks a year

Attacks ↓ **Demands** ↑ **Data Leaks** ↑

57x
Higher Global losses in 2021 compared to 2015

37x
Higher demands in 2021 compared to 2018

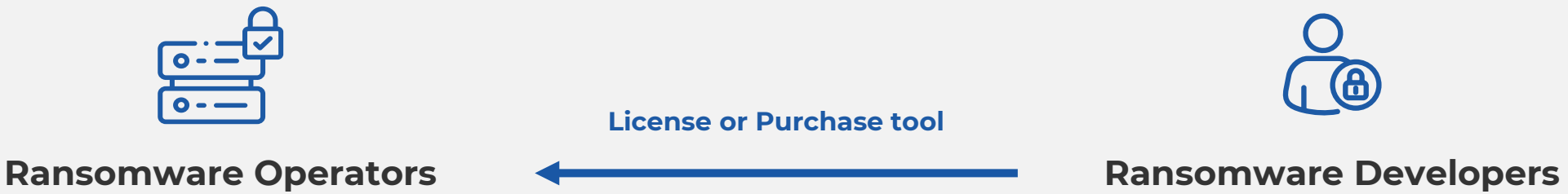


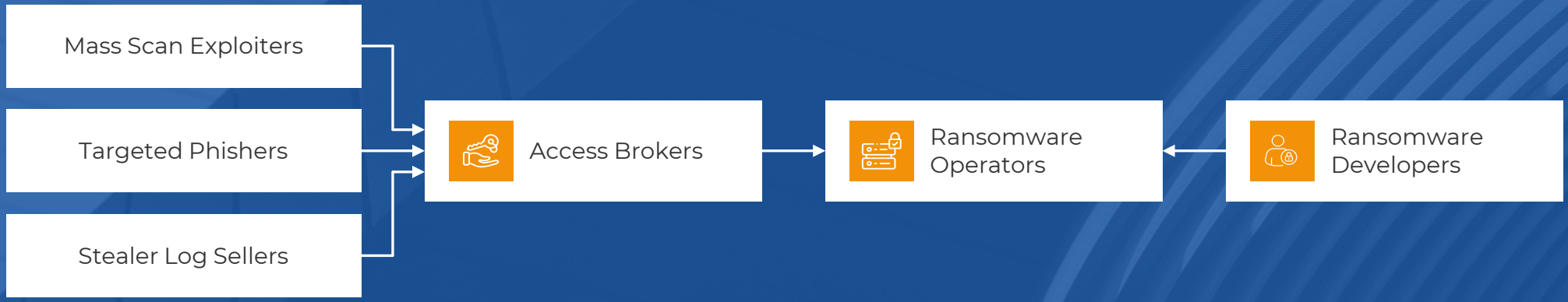
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
https://www.cloudwards.net/ransomware-statistics/

Frequency

Ransomware-as-a-Service

Develop Ransomware & Deploy as widely as possible





Ransomware
2020-2022

Colonial hack: How did cyber-attackers shut off pipeline
By Joe Tidy
Cyber reporter

10 May 2021

Insurance giant AON hit by a cyberattack over the weekend
By Lawrence Abrams

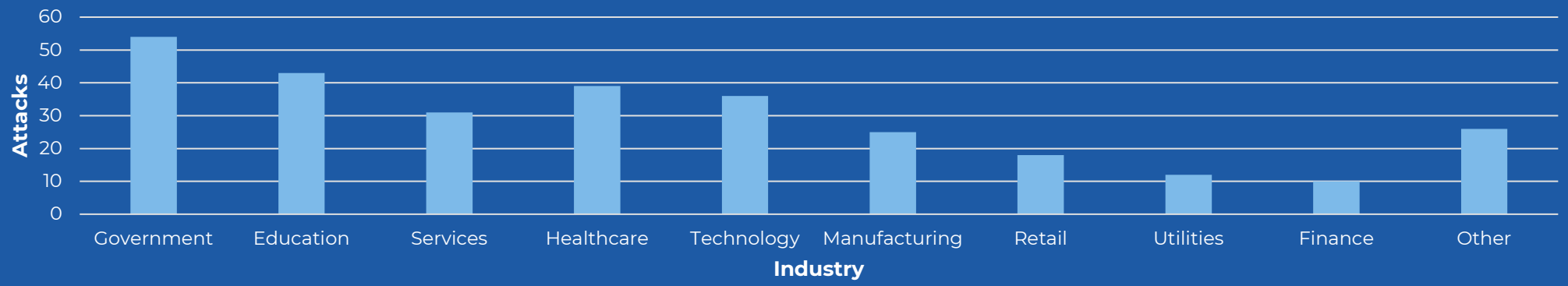
28 February 2022 10:39 AM

Meat giant JBS pays $11m in ransom to resolve cyber-attack

10 May 2021

Kaseya ransomware attack sets off race to hack service providers-researchers
By Joseph Menn

CNA Financial Paid $40 Million in Ransom After March Cyberattack
- Payment bigger than previously disclosed ransoms, experts say
- Malware tied to Russian cybergang sanctioned by U.S in 2019



https://www.blackfog.com/the-state-of-ransomware-in-2021/

What is being done

Ransomware

Government Intervention

- Law Enforcement Action

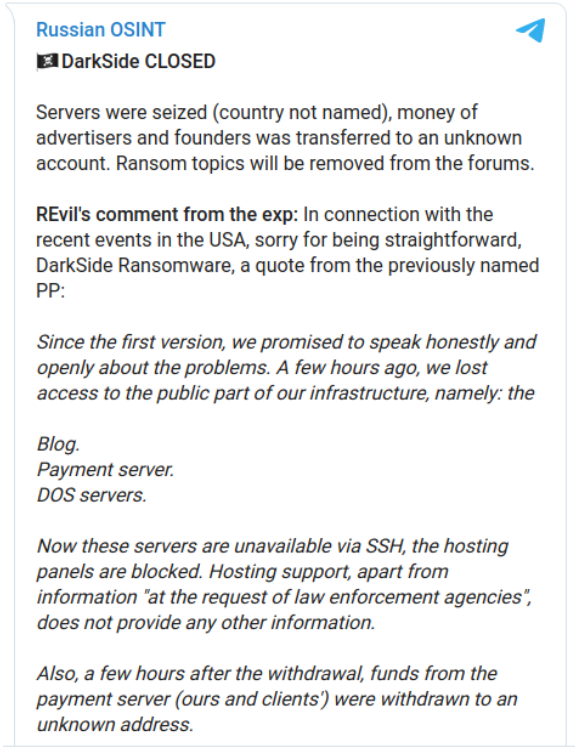
Arms Race

- New better detection and response tools

Insurance

- Aggregating data about attacks
- Improving methods of responding

Minimum Standards of Security....



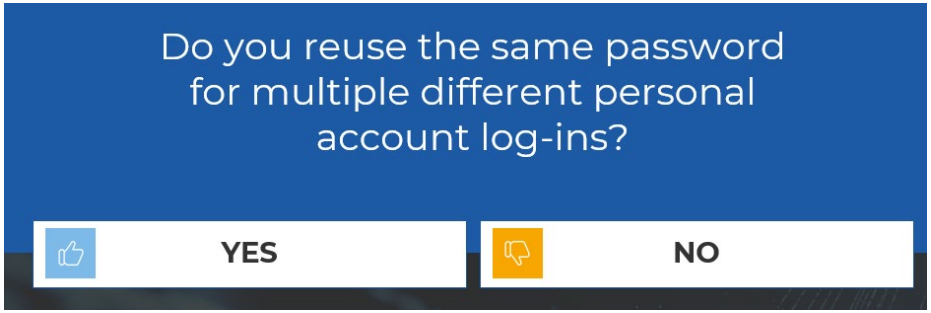
Ransomware

Minimum Standards

Multifactor Authentication

- Remote Working – password reuse
- Colonial Pipeline – Single Factor

24 Billion usernames and passwords stolen



Ransomware

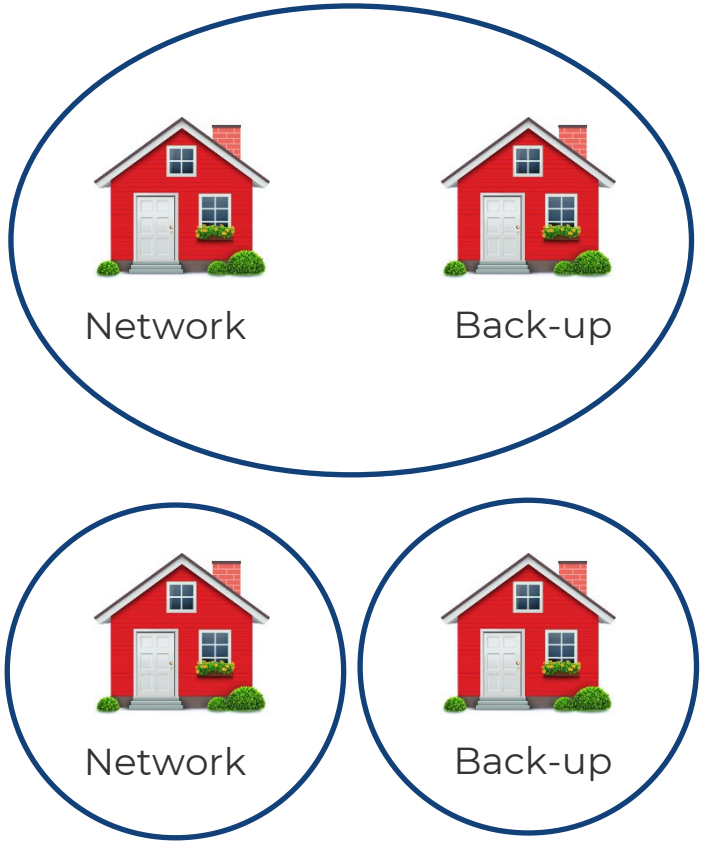
Minimum Standards

Multifactor Authentication

- Remote Working – password reuse
- Colonial Pipeline – Single Factor

Offline / Disconnected Backups

- Good backups, uninfected and regularly tested = no need to pay



Ransomware

Minimum Standards

Multifactor Authentication

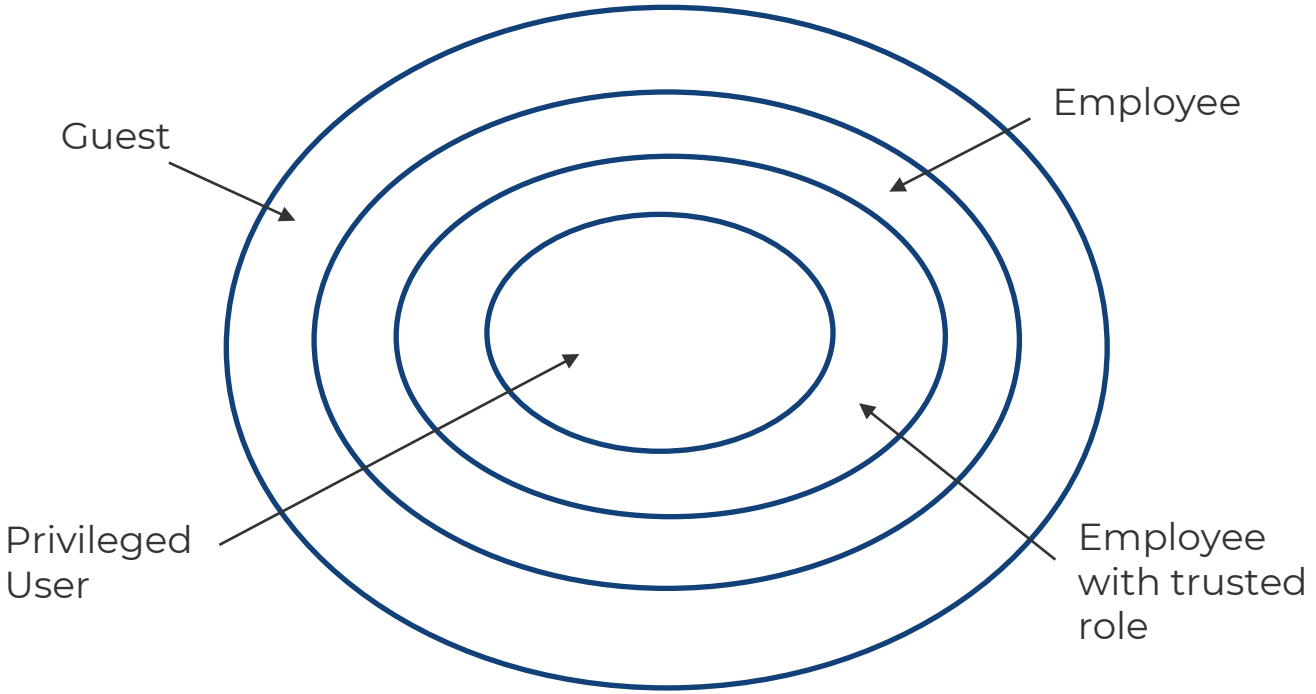
- Remote Working – password reuse
- Colonial Pipeline – Single Factor

Offline / Disconnected Backups

- Good backups, uninfected and regularly tested = no need to pay

Privileged Access Management

- Prevent the intruder gaining access to entire system



Ransomware

Minimum Standards

Multifactor Authentication

- Remote Working – password reuse
- Colonial Pipeline – Single Factor

Offline / Disconnected Backups

- Good backups, uninfected and regularly tested = no need to pay

Privileged Access Management

- Prevent the intruder gaining access to entire system

Endpoint Detection and Response

- Constant security at the edges of the network

Ransomware

Minimum Standards

Multifactor Authentication

- Remote Working – password reuse
- Colonial Pipeline – Single Factor

Offline / Disconnected Backups

- Good backups, uninfected and regularly tested = no need to pay

Privileged Access Management

- Prevent the intruder gaining access to entire system

Endpoint Detection and Response

- Constant security at the edges of the network

Regular Patching

- Once a vulnerability is public, outside-in scans can find those that have not patched

Almost none of these questions existed before 2018 on cyber application forms

Insurance

Minimum Standards

- Multifactor Authentication
- Offline / Disconnected Backups
- Privileged Access Management
- Endpoint Detection and Response
- Regular Patching
- Log and Monitor Abnormalities
- Anti-Spoofing controls – DMARC, SPF, DKIM
- Sandboxing suspicious emails
- Authenticate communications before changing bank details

Ask us anything

Within reason!

Some suggested questions:

- ❑ War Exclusions – how do they function when attacks appear to be coming from State Governments
- ❑ Property Damage – is it covered?
- ❑ How quickly will Artificial Intelligence change things?
- ❑ Should it be illegal to pay ransomware claims?