Cyber Update

NJCE

NEW JERSEY COUNTIES
EXCESS JOINT INSURANCE FUND

Pre-Renewal Update on Cyber Controls

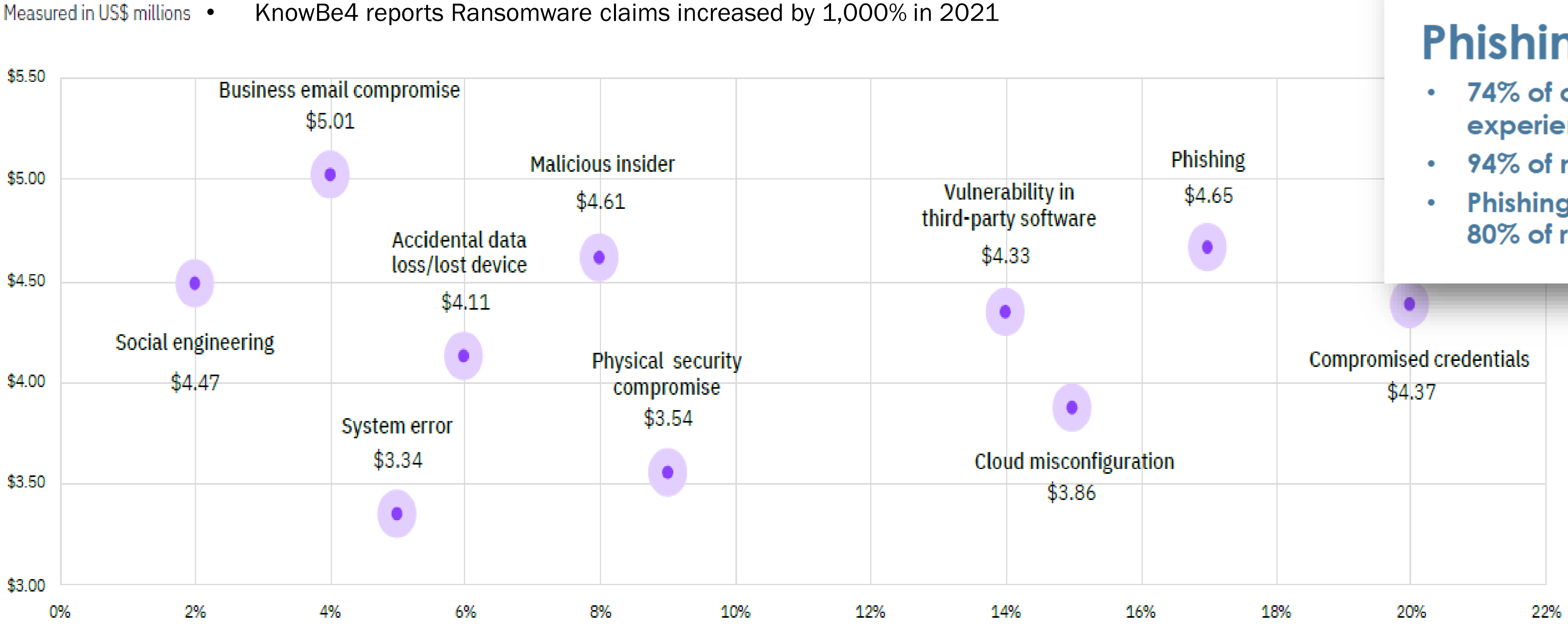
July 2022

What Are The Issues?

The Issues

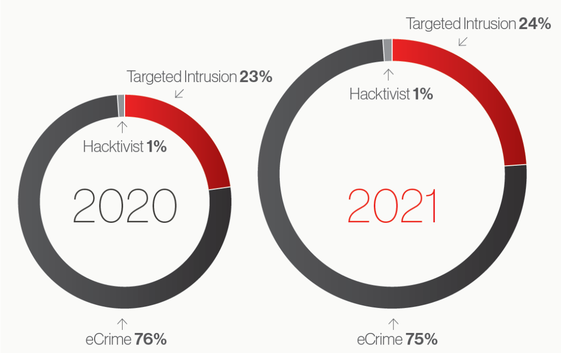
The Key Problem: Extortion

- A. M. Best reports: Cyber insurance industry loss ratio rose by 51% from 2019 to 2020, Ransomware claims rose 35% in 2020, which now account for 75% of all Cyber claims
- FireEye reports 41% of identified malware families in 2020 were new / previously unknown, showing the quick acceleration of attacker innovation
- IBM/Ponemon reports: 48% of breaches were caused by human error and system glitch, 20% of breaches were due to compromised credentials, 16% of breaches due to 3rd party vulnerabilities
- KnowBe4 reports Ransomware claims increased by 1,000% in 2021



Phishing

- 74% of organizations in the US experienced a successful phishing attack
- 94% of malware is delivered by email
- Phishing attacks account for more than 80% of reported security incidents



The Issues

287

Average number of days to identify and contain a data breach

The longer it took to identify and contain, the more costly the breach.

Data breaches that took longer than 200 days to identify and contain cost on average $4.87 million, compared to $3.61 million for breaches that took less than 200 days. Overall, it took an average of 287 days to identify and contain a data breach, seven days longer than in the previous report. To put this in perspective, if a breach occurring on January 1 took 287 days to identify and contain, the breach wouldn't be contained until October 14th. The average time to identify and contain varied widely depending on the type of data breach, attack vector, factors such as the use of security AI and automation, and cloud modernization stage.

$4.62m

Average total cost of a ransomware breach

Ransomware and destructive attacks were costlier than other types of breaches.

Ransomware attacks cost an average of $4.62 million, more expensive than the average data breach ($4.24 million). These costs included escalation, notification, lost business and response costs, but did not include the cost of the ransom. Malicious attacks that destroyed data in destructive wiper-style attacks cost an average of $4.69 million. The percentage of companies where ransomware was a factor in the breach was 7.8%.

20%

Share of breaches initially caused by compromised credentials

Compromised credentials was the most common initial attack vector, responsible for 20% of breaches.

Business email compromise (BEC) was responsible for only 4% of breaches, but had the highest average total cost of the 10 initial attack vectors in the study, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million).

What Minimum Controls Are Needed?

Cyber Controls

** The market is demanding certain cybersecurity controls be in place in order to provide full Ransomware coverage or even quote Cyber coverage at all. The requirements are typically required to be in place prior to binding; sometimes 30 days. **

Quote or No Quote

Multi-Factor Authentication (MFA): Applied for all remote access to the network, remote email, privileged users and off-network back-ups.

Back-Ups: All mission critical data and applications must be backed-up off-network or completely segmented.

- *Insurers are not yet discussing data stored by third parties (applications, vendors, etc.), but this will likely soon be part of the requirement.*
- *Some insurers are requiring some variation of the 3-2-1 Back-Up Rule, which is 3 back-ups, on 2 different types of media and 1 copy must be off-site.*

Endpoint Protection (EPP/EDR): Endpoint protection, detection and response.

- *Just having antivirus security at your endpoints is not enough; you must be able to detect the actual or potential threats in real-time and be able to respond.*

Other Key Underwriting Considerations

Employee Training: Employee training is a must. Insurers have not quite defined it yet, but the standard is 1 hour per year covering malware identification, password construction, identifying security incidents and social engineering attacks, with phishing testing.

Patching: Insurers will look at your patching cadence to see that all security updates (especially critical ones) are quickly applied. Insurers may also ask about your patch management procedures: How are you notified of available patches, and what procedure/timeline is used for implementing? Also be ready to confirm if you have remediated any instances of specific vulnerabilities, such as log4j (CVE-2021-44228).

Virtual Private Network (VPN): Most insurers are requiring VPNs used for remote access. In lieu of VPN, there are certain Remote Desktop Protocol (RDP) providers with strong security in place, but this may be a tough conversation with underwriters as they will have to refer these security questions to their cybersecurity consultants.

Check out the NJCE Cyber Task Force's Cyber Risk Management Program for more details of controls and policies.

Cyber Controls

Additional Minimum Controls

Password Strength: We all understand the importance of complex passwords, but it is critical these are unique from all other passwords each individual uses elsewhere in life.

Access Privilege and Segregation: Simple enough, each employee does not need access to the parts of the network for all other departments. With this in place, attackers may get into Jane Doe's account, but Jane Doe's account will not have access to other parts of the organization.

Encrypt Data: Encrypt your data, especially sensitive (financial, PII, PHI) so if you are breached or accidentally release data, the data is unusable.

Deep Web Scans: Organizations should utilize a service that constantly scans the deep web for your email addresses and passwords in known breaches and your organization's documents containing potentially sensitive information.

Incident Response and Business Continuity: Time is of the essence in attacks and can make all the difference. Have an incident response plan and regularly test it. Develop a business continuity plan to keep operations as high as possible during the event. These will help produce drastic differences in your total loss.

Vulnerability Scanning and Penetration Testing: Periodic Penetration Tests will help test the security you have implemented, while frequent vulnerability scanning will address vulnerabilities in your applications, which are frequently occurring.

Third Party Security Audits: Especially for some of your high-risk vendors (accounting, employee benefits, IT), utilize a security audit to ensure they are protecting your data and network like you would protect it yourself.

Security Operations Center (SOC): A 24/7 staffed security operations center.

Advanced Credential Management: Ensuring different credentials are used for back-ups and certain other segmented areas, different than the normal environment's administrator credentials. Also perform credential integrity checks against known breaches on a regular basis.

Back-Up Testing: Back-ups should also be tested for integrity on a regular basis (every 3 months).

Advanced Security Software: Utilize a network monitoring solution that alerts for suspicious or malicious behavior (such as SIEM).

Cyber Controls: Operational Technology (OT / ICS)

Minimum Controls for Operational Technology / Industrial Control Systems (OT / ICS)

Segmentation: OT/ICS environments should be segmented from other environments. This can be done virtually or physically.

Accounts/Credentials: No accounts, usernames or passwords should be the same as what is used on the regular business network.

Email and Web Browser: No web browser should be on the network, if possible. Only email access should be outgoing emails, not incoming.

Border: All network points need to be known and secured. Limit access to known IPs. No direct internet connection. Endpoint detection and response.