Jewelers Mutual®

EST 1913

October 25th, 2023

Cybersecurity Simplified: Staying Safe in the Digital Age

Presented by Grant Hansen

Agenda

Cybersecurity Simplified: Staying Safe in the Digital Age

1. State of Cybersecurity
2. Ransomware Attack - Demystified
3. Key Cybersecurity Measures
4. Cyber Education
5. Key Take Aways
6. References

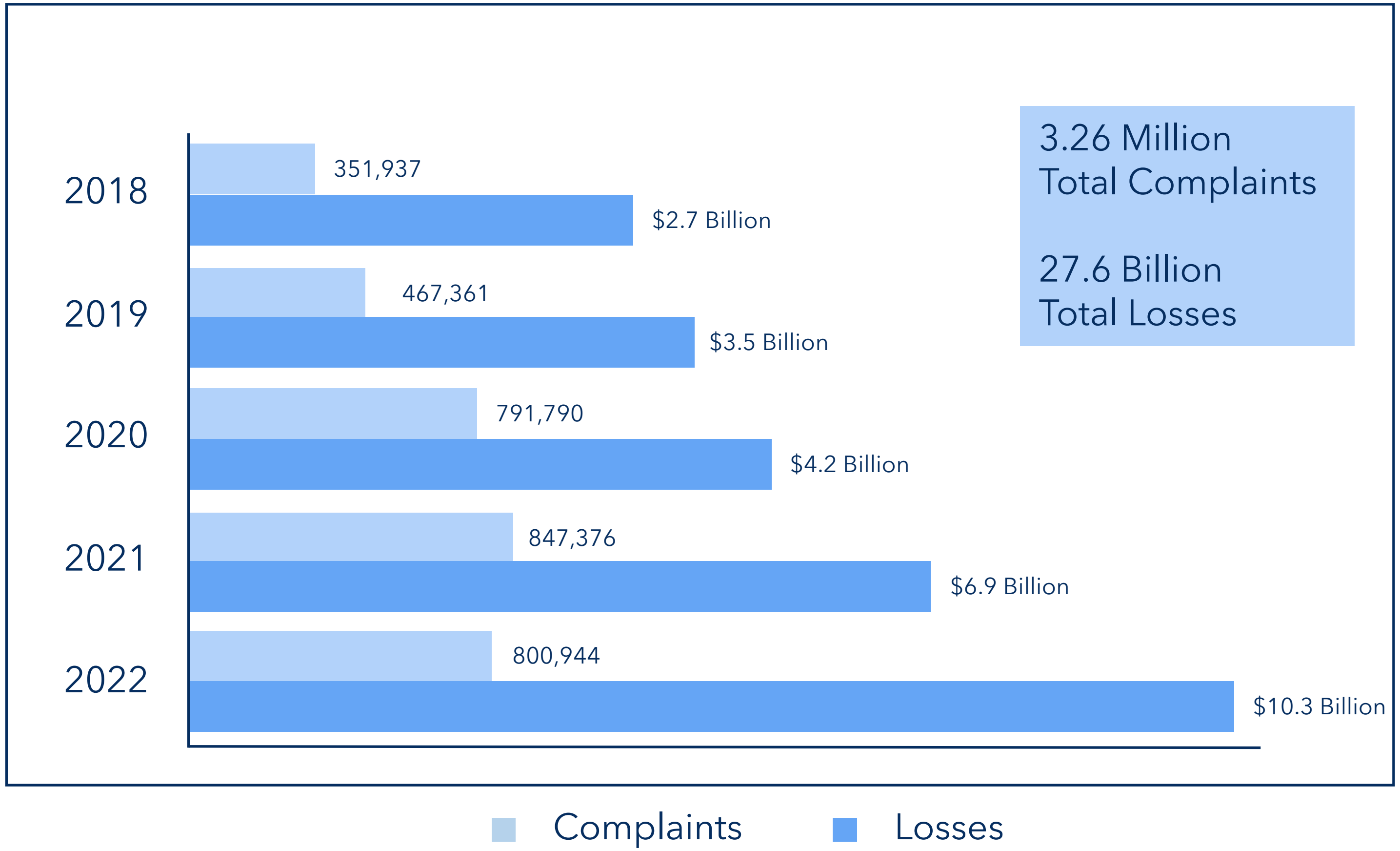
Section 1

State of Cybersecurity

State of Cybersecurity – What's in the News

- Recent Data Breaches
  - MGM
    - Ransomware Attack
    - Initiated via Social Engineering – Vishing
    - $100 million in cost – Covered by Cyber Insurance
  - Caesars
    - Ransomware Attack
    - Paid the Ransom ($15-30 million)
- Privacy legislation
  - No Federal privacy law yet!
  - Several states have enacted privacy legislation (understand how this impacts you)

State of Cybersecurity – What does the data say?



3.26 Million
Total Complaints

27.6 Billion
Total Losses

- Over the last five years, the Internet Crime Complaint Center (IC3) has received an average of 652,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.

	Complaints	Losses (Billions)	Avg Per Complaint	YOY Chg. Complaints	YOY Chg. Losses
2018	351,937	2.8	7,672		
2019	467,361	3.5	7,489	33%	30%
2020	791,790	4.2	5,304	69%	20%
2021	847,376	6.9	8,143	7%	64%
2022	800,944	10.3	12,485	-5%	45%

*Data provided by 2022 Internet Crime Report

State of Cybersecurity – Threat Actors

- Source of the Attack
    - 83% of breaches are initiated by external threat actors
        - Over 70% initiated by Organize Crime
        - Nation-State accounted for ~5%
    - Remaining - Internal threats, business partners and other

- Motivations
    - 97% are financially motivated
    - Remaining – Espionage, ideology and grudge

* Data provided by the 2023 Verizon Data Breach Report.

State of Cybersecurity – Types/Methods

- Top Attack Types – Data Breach
  - Credential Theft - 40%
  - Ransomware – 25%
  - Phishing – 12%
  - Exploit Vulnerabilities - 4%
  - Privilege Abuse - 4%
  - Backdoor Command and Control - 4%

- Top Attack Methods – Data Breach
  - Web Applications - 60%
  - Email – 30%
  - Carelessness – 15%
  - Desktop Sharing Software - 1%

* Data provided by the 2023 Verizon Data Breach Report.

State of Cybersecurity – SMB vs Large Enterprises

Small Business (Less than 1,000 Employees)	
Frequency	699 incidents, 381 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat Actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)

Large Business (More than 1,000 Employees)	
Frequency	496 incidents, 227 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat Actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor Motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)

* Data provided by the 2023 Verizon Data Breach Report for small business

State of Cybersecurity – Top Threats

- Social Engineering (Powered by Gen/AI)
- Ransomware
- Supply Chain
- Credential Theft

Section 2

Ransomware – Demystified

Ransomware - Demystified

- What is a Ransomware Attack?
  - Malware attack that locks a victim’s data or device and threatens to keep it locked, delete or release it

- Ransomware Attack Paths
  - Phishing
  - Visiting a malicious website – (drive-by downloads)
  - Vulnerable or mis-configured systems

Ransomware – Demystified

	Cyber Protections	MGM Breach
Delivery: Ransomware is delivered	Security Awareness, Anti-Malware Software, Access Control	Social Engineering (Vishing) of help desk facilitated reset of MFA tokens for privileged accounts
Command and Control (CC): Establish a connection with the threat actor's CC server to receive instructions.	Firewalls (URL Filtering, IPS, Monitoring/Incident Response	Once privileged account access was obtained, command and control are easily established
Credential Access: Malware continues with the attack by stealing credentials (Lateral movement)	Access Control, Monitoring/Incident Response	Attackers compromised MGMs Identity Infrastructure (Okta)
Locate and Encrypt: Ransomware will locate and encrypt/exfiltrate any data it has access to.	Monitoring/Incident Response	Non-public information is encrypted and most likely exfiltrated. MGM started taking systems offline
Extortion: Payment is demanded to release or decrypt the files back to the business.	Backups and Recovery, Cyber Insurance	MGM chose not to pay the ransom. Per MGM Cyber Insurance will cover the loss

Section 3

Key Cybersecurity Measures

Key Cybersecurity Measures – Must Haves

- Establish security-aware culture
- Have a plan to respond to an incident
- Establish relationship with trusted a partner
- Train your employees
- Ensure appropriate access
- Strong authentication controls (Multi-factor Authentication (MFA) is a must)

- Keep your systems up to date (Patch)
- Backup your data (Offsite, Immutable Copy)
- Reputable anti-malware solution
- Web filtering technology
- Encrypt your data
- Firewall (URL Filtering, AV, Remote Access, Firewall, Intrusion Prevention)
- Secure software development*

*If your organization develops its own software.

Section 4

Cyber Education

Cyber Education

- Jewelers Mutual recently launched two Cybersecurity awareness training modules.
  - Securing Digital Access
    - Password Development
    - Safeguarding Credentials
    - Use of Multi-factor Authentication
    - Data Protection
  - Cyber Deception Tactics
    - Social Engineering
    - Phishing
    - Business Email Compromise
    - Safe Use of Social Media

Sign up for FREE **here** or
scan the QR code below!

JewelersMutual.com/Academy

Section 5

Key Take Aways

Key Take Aways

- Understand the potential impact of a data breach like Ransomware or Business Email Compromise (Importance of Cyber Insurance)
- Cyber Attacks are not going away
- Small businesses are targeted more frequently
- Be aware of the source of attacks (External) and motivations (Financial)
- Threats will become increasing effective with the assistance of Generative A/I
- Assess your security posture against the "Must Haves"
- Training – Jewelers Mutual has free resources to assist

Section 6

References

References

- Verizon Data Breach Report
- Verizon Data Breach Report for Small Business
- Internet Crime Report 2022
- Privacy legislation tracker
- Technology and Cybersecurity Considerations

Jewelers Mutual®

EST 1913

Thank You

If you have any questions, please feel free to contact Grant Hansen at ghansen@jminsure.com