Cybersecurity in Missouri Municipalities

Brad Sandt, President & CEO
Cybersecurity for Local Government

• What are common cybersecurity risks?
• How vulnerable are Missouri Cities?
• What else to worry about besides a data breach?
• Where is your community vulnerable?
• How will you respond to a breach?
• How do we attack this problem?
Cybersecurity Risks

• Data Breach
• Accidental Data Loss
• Phishing/Spear Phishing
• Malware
• Ransomware
Cybersecurity Risks

• Data Exfiltration
• Common Vulnerabilities and Exposures (CVE)
• Remote Code Execution (RCE)/Privilege Escalation (PE)
• Account Takeover
• Supply Chain Attack
• Distributed Denial of Service (DDoS)
15 Top Threats in 2020

1. Malware
2. Web-based attacks
3. Phishing
4. Web application attacks
5. Spam
6. DDoS
7. Identity theft
8. Data breach
9. Insider threat
10. Botnets
11. Physical manipulation, damage, theft and loss
12. Information leakage
13. Ransomware
14. Cyberespionage
15. Cryptojacking

European Union Agency for Cybersecurity
Attack Techniques (June 2021)

- Malware: 40.8%
- Unknown: 25.1%
- Vulnerability: 9.5%
- DDoS: 7.6%
- Targeted Attack: 6.2%
- DDoS: 5.4%
- Account Takeover: 0.5%
- Misconfiguration: 0.5%
- Crypto scam: 0.5%
- Business Email Compromise: 0.5%
- Spam: 0.2%
- Malvertising: 0.1%
- Malicious Script Injection: 0.1%
- Defacement: 0.1%

Civic ITC
Frequency of Ransomware Attacks

2016

40s

2021

11s
Who’s Behind Data Breaches?

- **70%** Outsiders
- **55%** Organized Criminal Groups
- **30%** Internal Bad Actors
- **4%** Four or More Attacker Actions
- **1%** Multiple Partners
- **1%** Partners
95% of cybersecurity breaches are caused by human error.

Cybint

Phishing attacks account for more than 80% of reported security incidents.

CSO Online
Stats

- Average cost of a data breach is $3.86M in 2020 (IBM)
- Average lifecycle of a breach was 280 days (IBM)
- Personal data involved in 58% of breaches in 2020 (IBM)
- 64% of Americans have never checked to see if they were affected by a data breach (Varonis)
- 86% of breaches were financially motivated (Verizon)
Stats

• Average ransomware payment rose 33% in 2020 (Fintech News)
• 94% of malware is delivered via email (CSO Online)
• U.S. Ranks Highest with 18.2% of all ransomware attacks (Symantec)
• 20% of malicious domains used within one week of registering (Cisco)
• 30% of data breaches involve internal actors (Verizon)
• Since the pandemic began, the FBI reported a 300% increase in cybercrimes (IMC Group)
Not *If*, but *When*

- **Identify**  - How can they get in?
- **Protect**  - What tools do we have?
- **Detect**  - Can we locate intrusions?
- **Respond**  - How can we fix an intrusion if it occurs?
- **Recover**  - Do we have a plan in place to get back to normal?
SECURITY AWARENESS IS A CRUCIAL FACTOR FOR BUSINESSES IN 2020

- 50% of people receive at least one phishing email a day
- 97% of people cannot identify a phishing email when they receive one
- 53% of businesses have some form of security awareness training, meaning just under half have no training at all

https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic
WORKERS WOULD RATHER BE “NICE” THAN SAFE

1 in 5 share passwords over text or email

45% would share their computer with colleagues

EMPLOYEES DEMONSTRATE RISKY BEHAVIORS

55% admitted to clicking on links they didn’t recognize

49% have downloaded a web extension to their work device

DATA LOSS IS A REAL PROBLEM

7 in 10 respondents have accidentally deleted files

25% have lost data in G Suite or Microsoft Office 365
Simple Steps to Take

• Backup, Backup, Backup (air gap)
• Endpoint Protection/Anti-Malware
• Patch Systems (Windows/OSX/Network/Applications)
• Use Strong (and Different) Passwords/Multi-Factor Authentication
• Practice Safe Clicking
• Be Skeptical (Social Engineering)
• Create an Incident Response Plan
Simple Steps to Take

• General security awareness training.

• Simulated phishing campaigns.

• Third Party Assistance
Questions