Securing your business against hackers and thieves

Practical Solutions to Avoid Liability and Catastrophic Loss for Your Enterprise

ACC—Mountain West Chapter

Greenberg Glusker

INTRODUCTION

Will Fletcher—GC, Zasio Enterprises, Boise, Idaho

James Molen—Greenberg Glusker, Salt Lake City, Utah and Los Angeles

Tim Toohey—Greenberg Glusker, Bozeman, Montana and Los Angeles

Greenberg Glusker

Outline of Presentation

- Nature of risks
  - Bad actors
  - Ransomware and hacking
  - Spoofing and wire transfer fraud
- Potential harm to enterprises
  - Economic
  - Liability and litigation
  - Reputation/survival
- Practical Recommendations to avoid being a victim

Greenberg Glusker

Threat Actors and Harm

- Numerous Threat actors
  - Include state-sponsored actors
  - Spread wide net and communicate on dark web
  - Bots and automated techniques
- Target companies with vulnerabilities—regardless of size, industry sector
  - Bad actors do not know or care about size
  - Ransomware to extort cryptocurrency
  - A numbers game—looking for vulnerabilities

Greenberg Glusker

Varieties of Attacks

- Wide variety of techniques to gain access to systems
  - Individuals within organization
    - Deliberate actions of disgruntled employees
    - Carelessness
    - Phishing
  - “Brute force” attacks—guess passwords
  - “Credential stuffing” (exploiting password data from other attacks)
    - Billions of passwords and logins available on “dark web”
    - Bots automate attacks
    - Users re-use passwords
    - Even strong passwords may be vulnerable if re-used
  - Exploit local servers (vs. cloud) and vulnerable unpatched endpoints

Other Attacks

- Fake e-mails from officers
- Attempts to obtain credentials of employees
- Wire transfer fraud
  - Impersonation of a vendor/customer
  - Funds transferred to bank account controlled by hacker
  - Transactions rarely can be reversed
  - Company may still be liable to a vendor even if it is the victim

Greenberg Glusker

Vulnerabilities

Method of attack

- Hijack remote access (25%)
- Phishing e-mails (12.8%)
- Software Exploits (43.3%)
- Social Engineering (3.1%)

Or, put another way:

- User Action (29%)
- External Exposure (71%)
- Can be both!

Greenberg Glusker

Why do attacks happen to companies

- Lack of communication between IT and executives/legal
  - Overburdened IT personnel with limited budget
  - Systems outdated (e.g., Exchange servers) or unpatched
  - IT, executives and legal do not speak the same language
  - Security not a priority

"It can't happen to us because we are too small/obscure/don't have personal information"

Greenberg Glusker

Consequences of attack

- System locked up/Ransomware
  - To pay or not to pay dilemma (and laws)
- Disruption to operations
- Key documents (e.g., engineering drawings) unavailable
- IT burdened and require outside help
- Executive energies deflected to attack
- Employee morale
- Client/customers—concerns and communication challenges
- Expense
- Cybersecurity insurance may pay some costs

Greenberg Glusker

Incident Remediation = $$$

- Forensic examination
- IT system remediation
- Legal costs
- Communication to employees and customers/clients
- Compliance with data breach notification laws
- All states (including Idaho, Montana, Utah, Wyoming)
- Laws may require notice to individuals if “personal information” compromised
- Attorney general/agency notifications in some states
- Some costs may be covered by a suitable insurance

Greenberg Glusker

Lawsuits

- Variety of theories—negligence, California Consumer Privacy Act, other laws
- September 2024 “23 and ME” class action settlement for $30 million
- Genetic data regarding Jewish and Chinese users exposed from testing
- Hackers used “brute force” (trial and error) attack and “credential stuffing” (automated injection of username/password pairs)
- Lawsuits from customers/clients and regulatory authorities (Canada, UK)

How to Avoid Being a Victim

- Know what data you collect and know where it is stored
- Implement all system patches (can be time consuming)
- Executives and legal prioritize security with IT and provide it adequate resources
- Eliminate vulnerable legal systems (e.g., local servers)
  - Move to the cloud (AWS etc.)
- Implement password management rules and don’t reuse passwords
- Use password manager and offer it to employees for use at home
- Use 2FA (two factor authentication)
- Control all access points to the systems
- Adequate anti-virus (depending upon size of enterprise)

Greenberg Glusker

How to Avoid Being a Victim

- Train your employees regarding security issues
  - Look at e-mails from clients/executives for suspicious characteristics
  - Proper wire transfer protocols
  - Don’t click on executable files
- Implement mandatory password changes
- Backups not accessible to the Internet or in the Cloud
- Run software to monitor attempted logins
- Purchase adequate cybersecurity insurance
  - Consult and use a knowledgeable and experienced broker

Greenberg Glusker

Questions

Greenberg Glusker

Contact Information

Greenberg Glusker