Welcome to Tech Exchange 2021

How to Avoid Becoming a Victim in Your Own Cybersecurity

HORROR STORY

Cybersecurity has reached a "Crucible of Crisis"

Gift Card Scam - $500

Payroll Fraud - $150,000

Invoice Manipulation - $342,000

Crucible of Crisis – Statistics

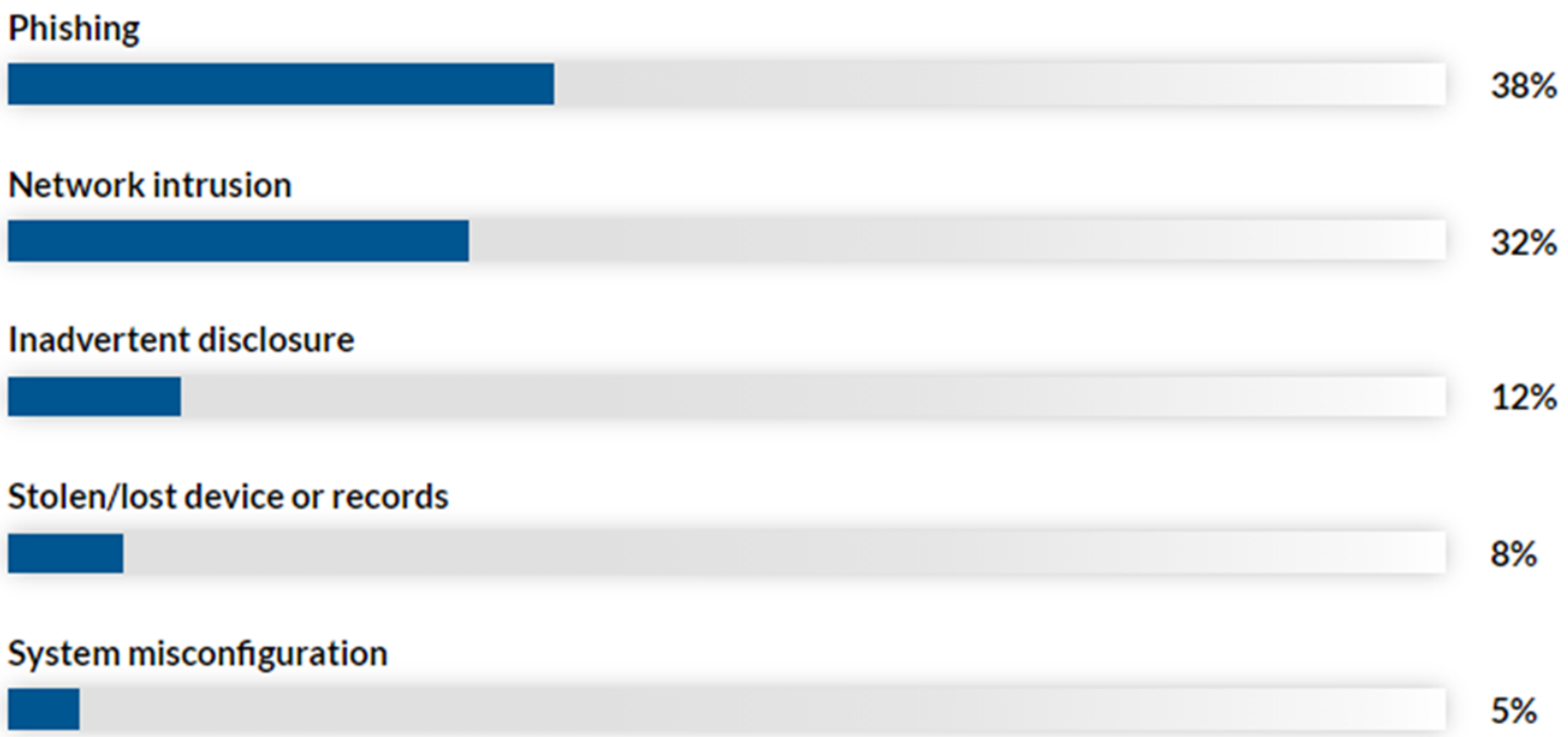
- Every 11 seconds, a U.S. business falls victim to a ransomware attack
- Malware use increased 358% in 2020 compared to 2019
- Ransomware increased 966% in June 2021 compared to June 2020
- 36 billion records exposed in first three quarters of 2020
- 86% of data breaches in 2020 were financially motivated
- Over 50% of all cyberattacks target small to medium businesses (SMB)
- 60% of SMBs that suffer a hacking or data breach fold within six months
- **Cybercrimes cost the world nearly $600 billion a year – that's 0.8% of global GDP**

Crucible of Crisis – Costs

- JBS USA: meat company; May 30, 2021 –paid $11 million ransom
- Colonial Pipeline: Oil & Gas; May 7, 2021 – paid $4.4 million ransom
- KIA Motors: Car manufacturer; February 2021 – believed to have paid $11 million ransom
- Buffalo Public Schools: March 12, 2021 – shut down the school of 34,000 students
- CNA Financial: U.S. Insurance Carrier; March 21, 2021 – Paid $40 million ransom
- ExaGrid: backup storage company; May 4, 2021 – paid $2.7 million ransom

Crucible of Crisis – Methods Used

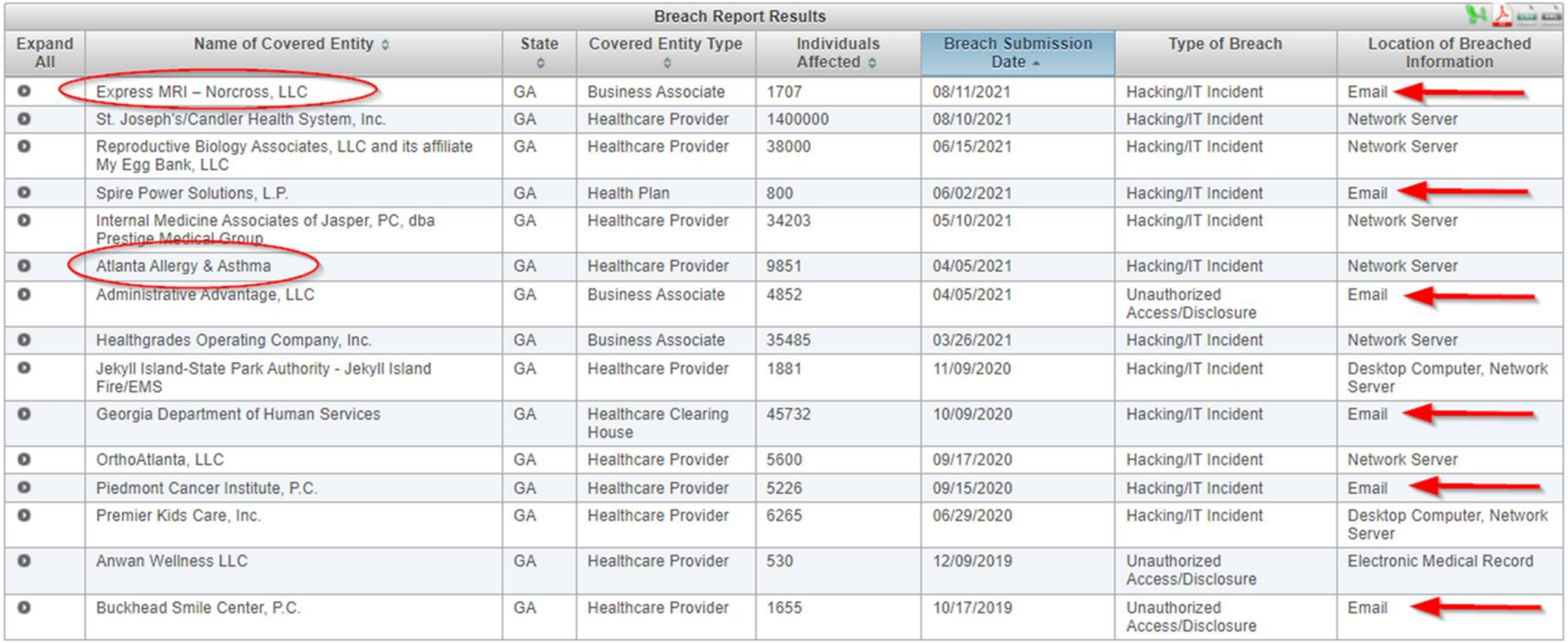
Most common cyberattacks experienced by US companies in 2020



Crucible of Crisis – Small Companies too

This list is from **ocrportal.hhs.gov** where the government shows WHO was hacked.

Note how many small business there are and how many involve email.



Breach Report Results

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	Express MRI – Norcross, LLC	GA	Business Associate	1707	08/11/2021	Hacking/IT Incident	Email
●	St. Joseph's/Candler Health System, Inc.	GA	Healthcare Provider	1400000	08/10/2021	Hacking/IT Incident	Network Server
●	Reproductive Biology Associates, LLC and its affiliate My Egg Bank, LLC	GA	Healthcare Provider	38000	06/15/2021	Hacking/IT Incident	Network Server
●	Spire Power Solutions, L.P.	GA	Health Plan	800	06/02/2021	Hacking/IT Incident	Email
●	Internal Medicine Associates of Jasper, PC, dba Prestige Medical Group	GA	Healthcare Provider	34203	05/10/2021	Hacking/IT Incident	Network Server
●	Atlanta Allergy & Asthma	GA	Healthcare Provider	9851	04/05/2021	Hacking/IT Incident	Network Server
●	Administrative Advantage, LLC	GA	Business Associate	4852	04/05/2021	Unauthorized Access/Disclosure	Email
●	Healthgrades Operating Company, Inc.	GA	Business Associate	35485	03/26/2021	Hacking/IT Incident	Network Server
●	Jekyll Island-State Park Authority - Jekyll Island Fire/EMS	GA	Healthcare Provider	1881	11/09/2020	Hacking/IT Incident	Desktop Computer, Network Server
●	Georgia Department of Human Services	GA	Healthcare Clearing House	45732	10/09/2020	Hacking/IT Incident	Email
●	OrthoAtlanta, LLC	GA	Healthcare Provider	5600	09/17/2020	Hacking/IT Incident	Network Server
●	Piedmont Cancer Institute, P.C.	GA	Healthcare Provider	5226	09/15/2020	Hacking/IT Incident	Email
●	Premier Kids Care, Inc.	GA	Healthcare Provider	6265	06/29/2020	Hacking/IT Incident	Desktop Computer, Network Server
●	Anwan Wellness LLC	GA	Healthcare Provider	530	12/09/2019	Unauthorized Access/Disclosure	Electronic Medical Record
●	Buckhead Smile Center, P.C.	GA	Healthcare Provider	1655	10/17/2019	Unauthorized Access/Disclosure	Email

What are the odds of getting caught?

The likelihood of detecting and prosecuting the perpetrator of a cyberattack in the US is 0.05%

(World Economic Forum, 2020)

That's 1 in 2000!

There is a new kid in town...

KILLWARE

Killware – a type of malware that is being deployed with the sole intention of causing physical harm or death.

- Water plants
- Food supplies
- Electrical grids
- Hospitals
- Airports
- Public transportation
- Arenas (ballparks, concert halls, etc.)

So…what are we supposed to do?

First things first – Cybersecurity starts at the top

Security is a:

- people problem
- process problem
- technology problem

A good leader:

- Knows the way
- Goes the way
- Shows the way

It is YOUR responsibility to usher in a culture of security

Pooh Bear was a hacker – he understood the power of the honey pot.

Honey pots attract hackers because they:

- Are easy to hack
- Have lots of useful / valuable information

90% of ALL breaches start with email

Common hacking targets:

- Public clouds (Azure, AWS, Rackspace, Google)
- Small businesses
- Financial institutions
- Healthcare providers
- Insurance companies

There's a saying in the hacker community…

"Hackers don't break in; they log in."

- Bogus websites
- Email links
- Reused passwords (81% of passwords are used in multiple sites and systems)
- Phishing scams

Protecting Office 365 – Email Platform

- Microsoft has developed a policy-based approach to security – it is turned off by default

- MIS has developed 22 essential security policies to protect Office 365

- New threats are continuously discovered – policies are iterative.

Protecting Office 365 – Cell Phones (MDM)

Only available to O365 customers

Used to protect cell phones

- Allows company to define acceptable use of cell phones
  - Application deployment
  - Access control
  - Device encryption
  - Prevents the use of jail broken devices

Microsoft Intune

Protecting Office 365 – DMARC

Domain Message Authentication Reporting and Conformance

- Tells the world how to handle unauthorized use of your email domain
- Fights:
  - Email compromises
  - Phishing
  - Spoofing
- Visibility - See who is sending email using your domain
- Delivery – ensures that your emails are delivered and not marked as spam

Protecting Office 365 – Artificial Intelligence

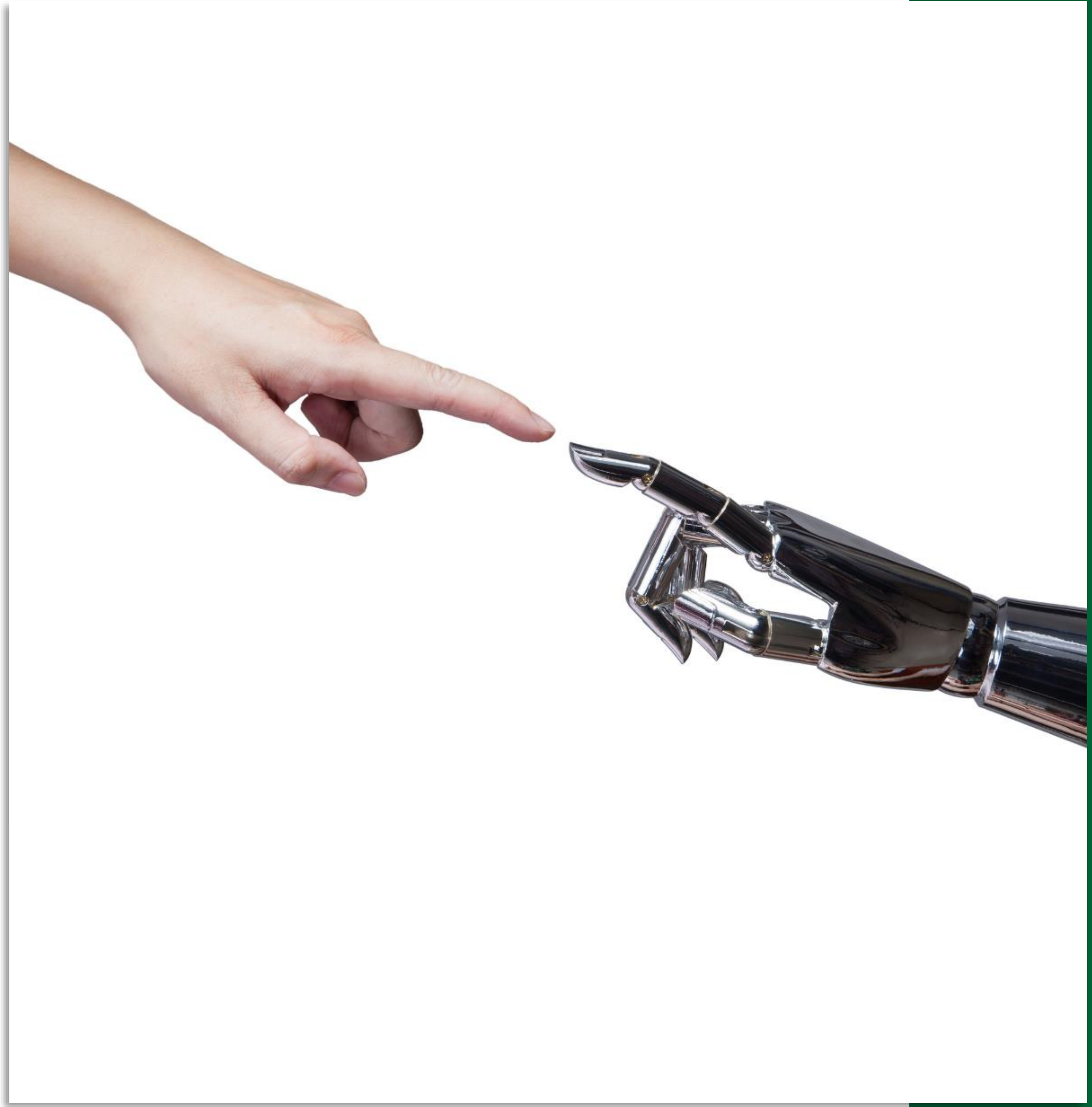
Scans each email using all the techniques we try to teach end users:

- Lookalike domains
- Language patterns
- Fake links
- Social graphing

Places a banner at the top of each email:

- **Red = bad**
- **Yellow = caution**
- **Gray = good**

Shows / trains users to spot malicious emails



Protecting Office 365 – Summary

- ✓ Apply security policies to protect the platform
- ✓ Use MDM to protect mobile devices
- ✓ Implement DMARC to authenticate email and provide reporting
- ✓ Use Artificial Intelligence to help users stop phishing / fake emails

Let’s Talk About the Role of Insurance

Insurance is a form of risk transference. Here is a checklist of items to discuss with your insurance agent:

- Phishing
- Social Engineering
- Invoice Manipulation
- Forensic Work
- Business Interruptions
- Cover for Extortion and Blackmail
- Loss of Data and Restorative Work
- Litigation Coverage
- Regulatory Coverage
- Communication and Notifications (breach notification)
- Credit Monitoring and Review
- Liability for Media Issues
- Liability for Breach of Privacy and Compliance

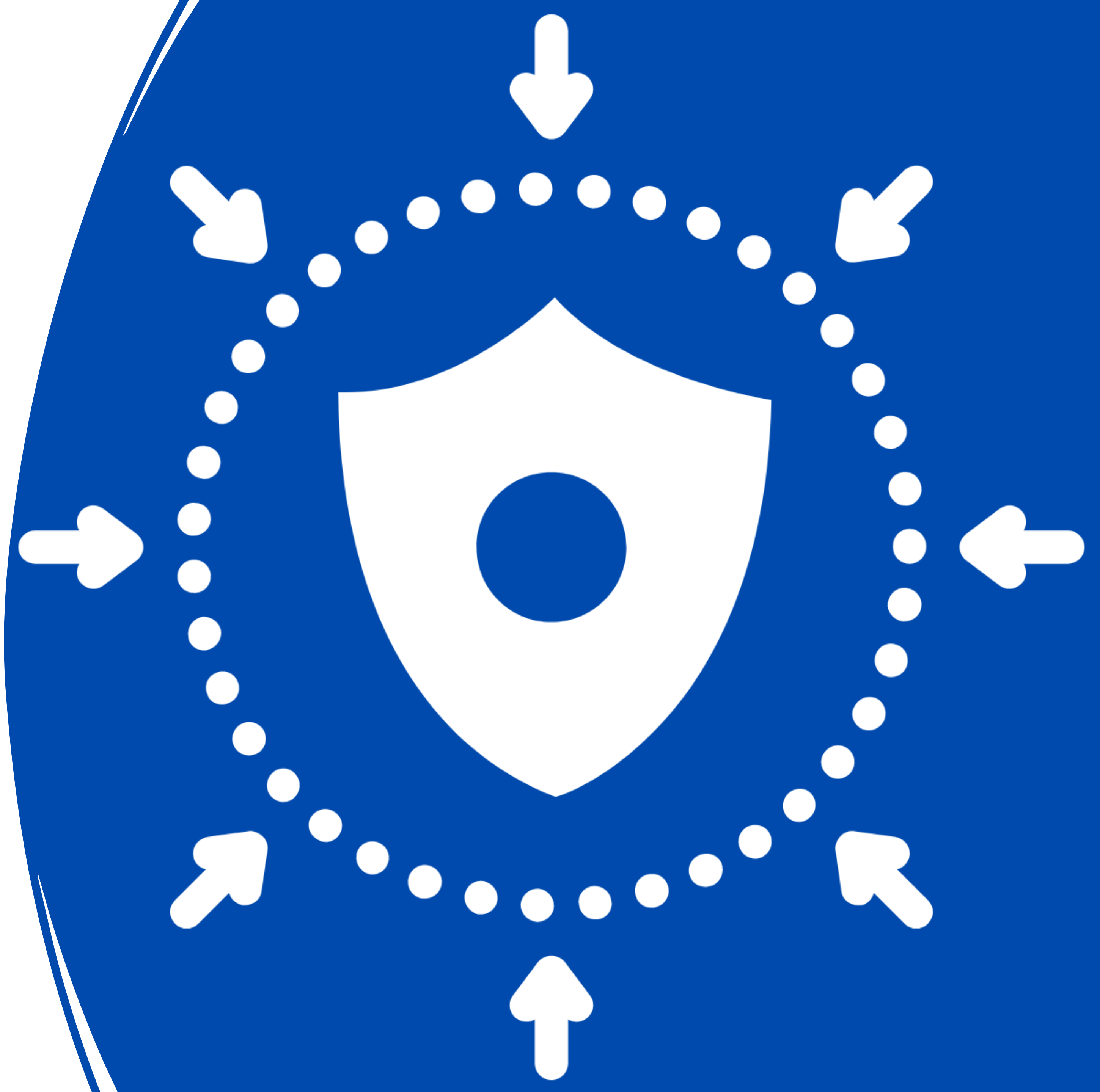
Insurance Underwriting Requirements:

Technical:

- Multifactor Authentication
- MDM for Cell Phones
- EDR / Nextgen Antivirus
- Encrypted Backups
- Annual Vulnerability Assessment

Administrative:

- User Security Training
- Finance Controls
- Incident Response Plan
- Risk Analyses
- Disaster Recovery Plan



Frameworks = Forgiveness

Two MAIN cybersecurity frameworks:

- **NIST 800-53 – security control driven**
- ISO 27001 – less technical / more risk focused

States are starting to provide safe harbor for companies that have implemented a recognized cybersecurity framework:

- Ohio
- Utah
- Connecticut

If you have a fully implemented cybersecurity framework (physical, technical and administrative) and something happens, then your company will be held harmless.

What Has MIS Done in the Past 18 months to Help Keep You Safe?

- Our technical staff has obtained 95 certifications
- Completed the SOC 2 Type 2 certification process
- Performed network and micro segmentation for all our support tools
- Deployed new firewalls for ALL customers that support the latest cybersecurity standards

What Has MIS Done to Help Keep You Safe? continued

- **Developed / implemented:**
  - Microsoft 22 security policies
  - Microsoft event security monitoring best practices
  - 2FA on ALL tools used by our internal staff
  - A disk encryption process that escrows the encryption key
  - Policies and procedures for:
    - Microsoft Intune (MDM)
    - DMARC monitoring and reporting
    - Artificial Intelligence email protection product
- **Developed & documented both a Code Red and Significant Event process**
- **Created and implemented a process for executing security tabletop exercises within each of the support teams.**

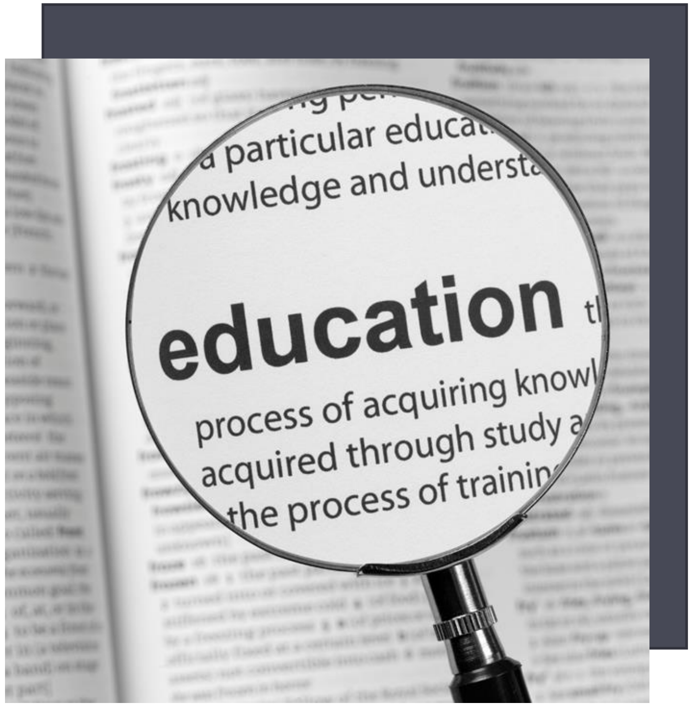
Cybersecurity Next Steps...

MIS consistently educates and informs our clients

- ✓ Monthly Newsletters
- ✓ Account Manager Update Emails
- ✓ Security Alerts

Technology Business Review /Cadence Calls

- ✓ Alignment
- ✓ IT Roadmap
- ✓ Manage Risk
- ✓ Future Prepare



MIS

Connect with Us!

facebook.com/
missolutions

linkedin.com/
company/mis-solutions

@MISsolutionsIT