Cybersecurity Webinar:

Addressing cyber risk & data protection

Presenters

Furney Brown

Alex has over twenty five years of information technology audit, technology regulatory control compliance, and system integration project experience. Alex has extensive experience in the assessment of technology risk and evaluation of IT controls in support of IT security regulatory compliance engagements (e.g. HIPAA/HITECH and Sarbanes-Oxley). In addition, Alex has extensive experience in working with various IT security control frameworks (e.g. NIST 800, ISO 27001/27002, COBIT, HIPAA, FERPA). Alex's industry experience includes: Government, Higher Education, K-12 Education, Healthcare, and Manufacturing. Alex holds a B.A. from North Carolina Agricultural and Technical State University.

Jennifer Fiebelkorn

Jen has over thirteen years of information security, control and IT audit experience. Jen's experience includes information systems general controls reviews, GLBA/privacy compliance, SOX 404 IT compliance, application reviews, and SOC reviews. Her industry experience includes: public sector, private equity, higher education, healthcare, and financial institutions. Jen holds a B.S. in telecommunications and information studies with a minor in computer science, with a specialization in information systems, from Michigan State University.

Overview of today's discussion

- Current environment/events
- How to prepare for next cyber attack
  - Recommendations
  - Best practices
- Q&A

Current Environment

Security Breaches Continue….

Hackers exploited vulnerability in Superion's Click2Gov Utility Bill Pay Systems affecting government entities across the U.S.

Over 20,000 records from eight cities in five different states have been offered for sale on the dark web.

City payment services downed in cyber attack

Officials refunded late charges related to downed services.
System was suspended deliberately to mitigate damage

Phishing cyberattack used against Florida city

Officials tricked into thinking email from bad actor was legitimate.

City officials confirmed they had paid the faux contractor

City communications hit in ransomware cyberattack.

Officials remained uncertain about personal information breach

Online payment systems affected; 911 services remained unaffected

Security Breaches Continue….

JP Morgan Chase Bank Admitted Leaking Sensitive Data of its Customers

AUGUST 17, 2021 DISSENT

NC: Hackers Steal Critical Customer Data From Bank Of Oak Ridge

JULY 11, 2021 DISSENT

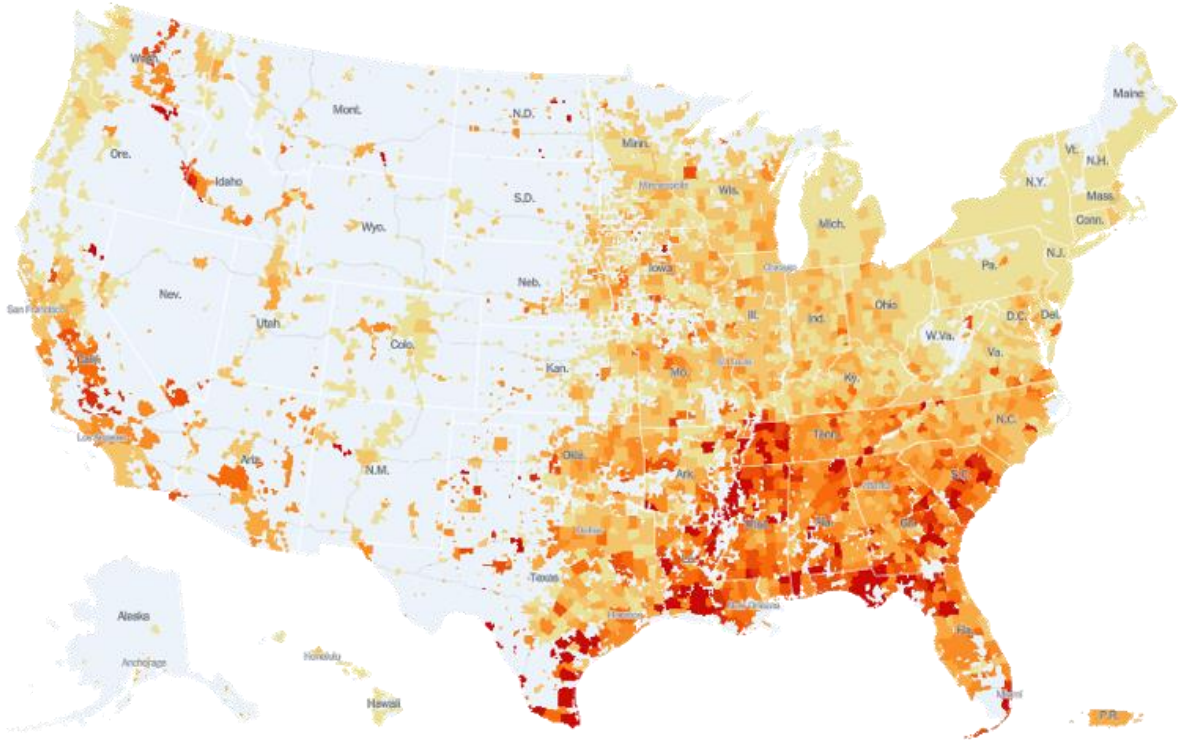
AmeriFirst Warns Customers of December Data Breach

APRIL 30, 2021 DISSENT

Mogin Rubin writes: The personal loan information of certain #AmeriFirst Financial, Inc., customers have been compromised, according to the bank's "data security incident" notification. AmeriFirst said it discovered the breach on April 12, 2021, which infiltrated the bank's data storage from Dec. 2 to Dec. 10, 2020. Read more on The National Law Review.

And Even In Today's News

COVID Pandemic Continues to Surge

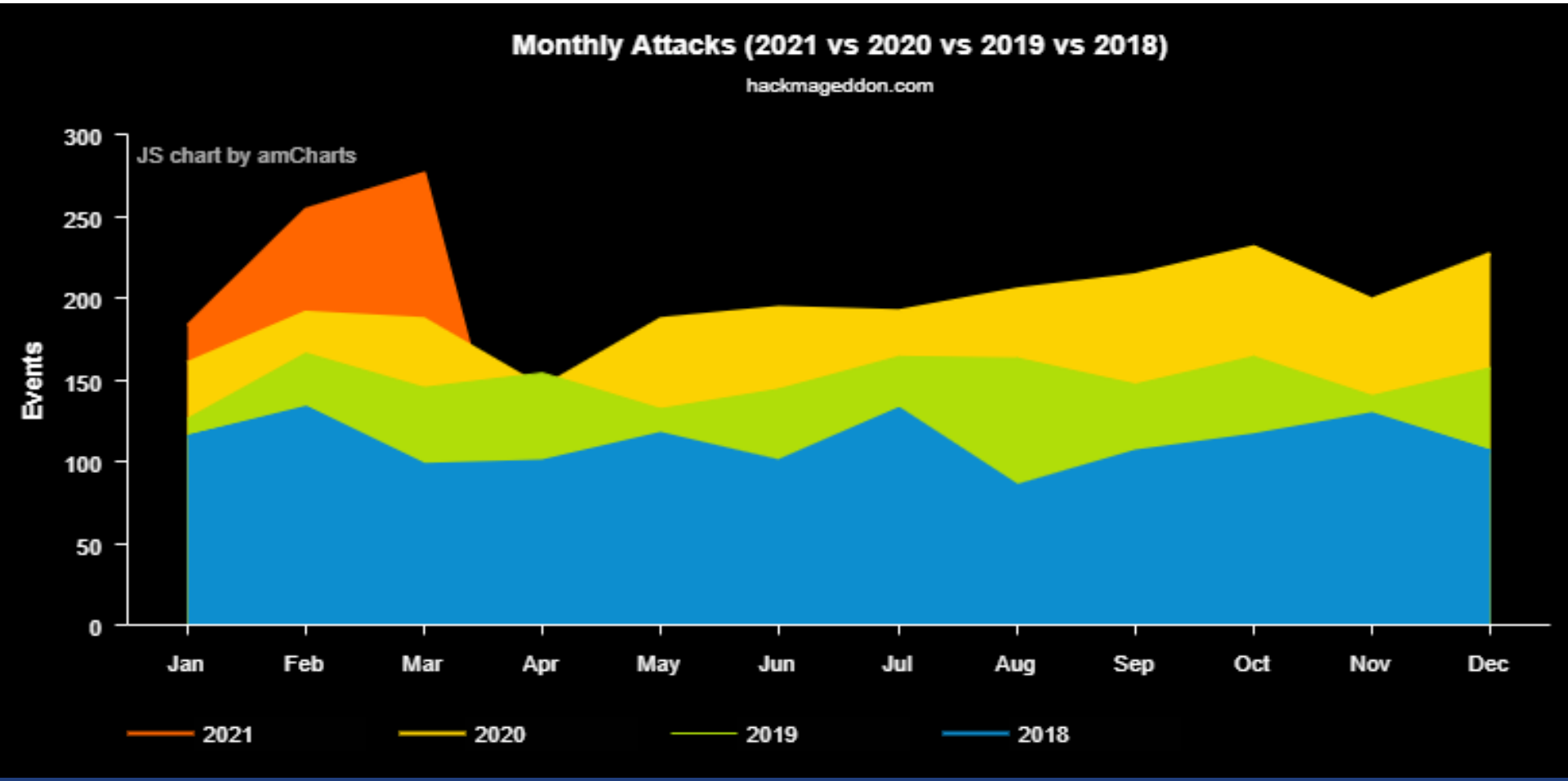


COVID 19 has added a new challenge to IT security. Below are a few examples

- Increase number of remote users
- High demand for remote connectivity
- Risk of data due to user's remote working space (e.g. Zoombombing
- User's technology (e.g. home router)

Cyber Attack Trends

Cyber attacks increased during COVID pandemic



Increase in Attacks due to COVID-19

Google says its averaging about **18 million daily malware and phishing emails** related to COVID-19 scams just daily. That's on top of the more than 240 million daily spam messages it sees related to the novel coronavirus, the company says.

In the midst of the global COVID 19 pandemic that has impacted businesses across the county as well as our daily lives, hackers have seized this opportunity for their personal gain.

Remote work applications like Zoom, Skype, WebEx are popular themes of phishing lures. This increase has exposed a number of organizations to vulnerabilities from social engineering (e.g. Phishing).

Cyber Attack Trends

1. Malware Exploitations

2. Web Attacks (sites and applications)

3. Phishing Attempts

4. Ransomware Attacks

5. Data Loss (Hardware, USB, Emails, etc.)

Cybersecurity Trends

Data Breach Stats

4.1 Data breaches exposed 4.1 billion records in the first half of 2021.

71% 71% of breaches were financially motivated and 25% were motivated by espionage.

2,244 Hackers attack every 39 seconds, on average 2,244 times a day.

314 The average lifecycle of a breach was 314 days (from the breach to containment).

48% 48% of malicious email attachments are office files

1 in 36 1 in 36 mobile devices had high risk apps installed.

Understanding the Why

- 76% of breaches were financially motivated.

  Most cybercriminals are motivated by cold, hard cash. If there's some way they can make money out of you, they will.

- Most attacks are opportunistic and target not the wealthy or famous, ***but the unprepared***.

- Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12%.

- Over a quarter (28%) of attacks involved insiders. The insider threat can be particularly difficult to guard against—it's hard to spot the signs if someone is using their legitimate access to data for nefarious purposes.

What are attractive targets to hackers?

- Security is **NOT** a top (or well- funded) priority
- **High amount of sensitive information maintained (e.g. financial information, medical records, student records)**
- **Successful attempts with prior attacks**
- **Old outdated technology**
- **Untrained employees**

Prepare for Next Cyber Attack

Approach to combat cyber threats

To keep hackers from exploiting all-too-common vulnerabilities, it takes a strong and coordinated defense that includes three major controls: people, process, and technology.

People

End users are your first line of defense from attacks. With the best intentions to provide fast service, employees may click on links or attachments in phishing emails in an effort to fulfill seemingly legitimate requests. But doing so enables hackers — unbeknownst to you — to install malicious software, request credentials such as passwords and security questions and answers, and initiate wire transfers.

Process

As threats constantly evolve, your processes to detect and resolve new threats must evolve as well. Patches to operating systems and third-party applications, for example, must be rigorously maintained to protect against the latest vulnerabilities. Your recovery planning process, too, needs to evolve to adequately address the increased new threats, such as ransomware.

Technology

While IT supports and facilitates your operations, it also must secure sensitive data and information entrusted to your organization. Strong controls are critical, whether you manage your IT organization in-house or outsource. You must ensure, not assume, vendor processes and controls align with the latest security protocols and your organizations and stakeholders' expectations.

People

People

- Dedicated individual or team responsible for Cybersecurity
- User access administration (new, changes, terminated)
- Access to systems and data on a need-to-know basis
- Train management and staff on cyber threats and best practices, company policies, etc.
- Strong passwords practices and requirements, including dual factor
- Managing third-party access

People are your first line of defense from attacks.

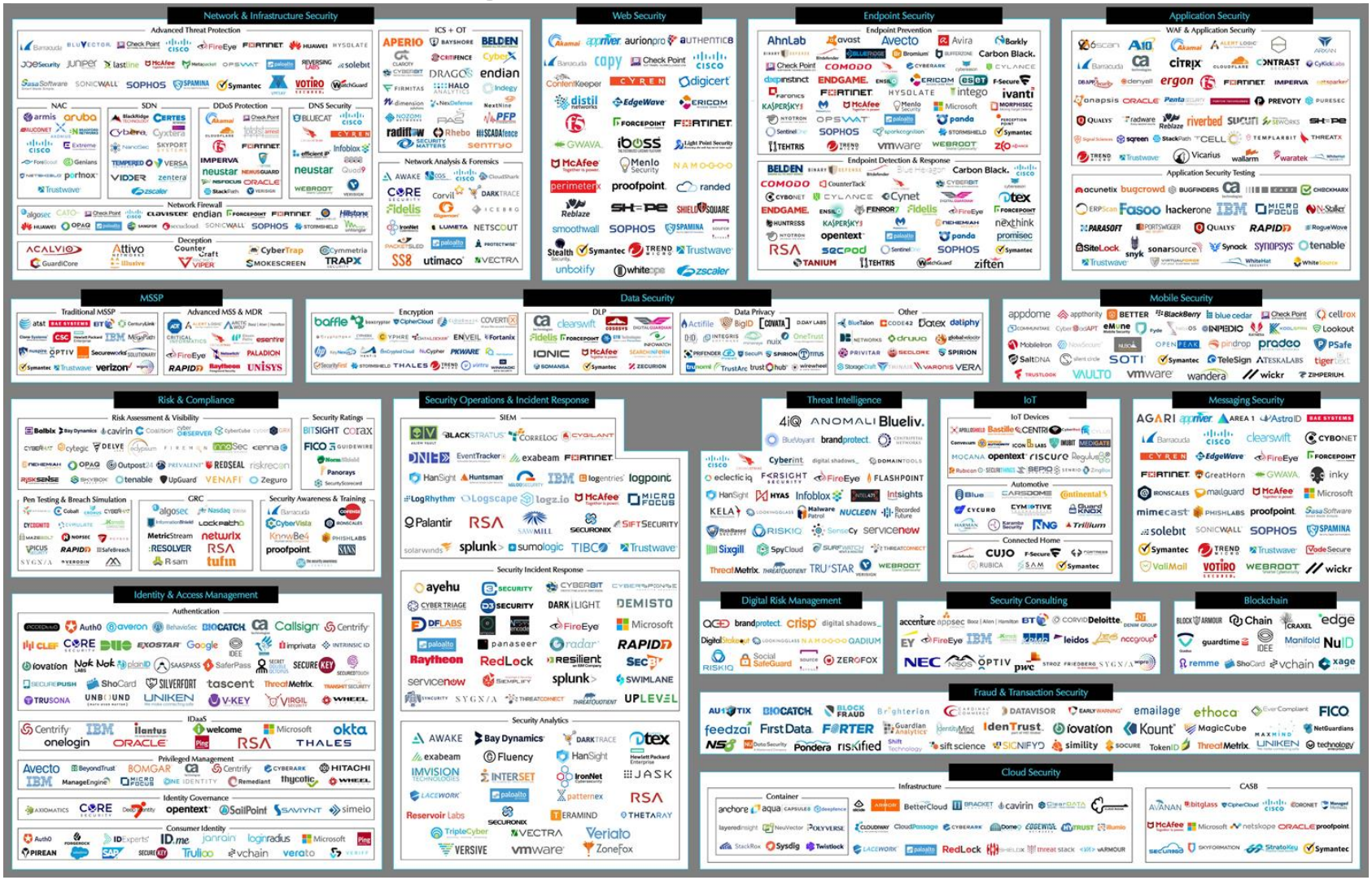
Process

Process

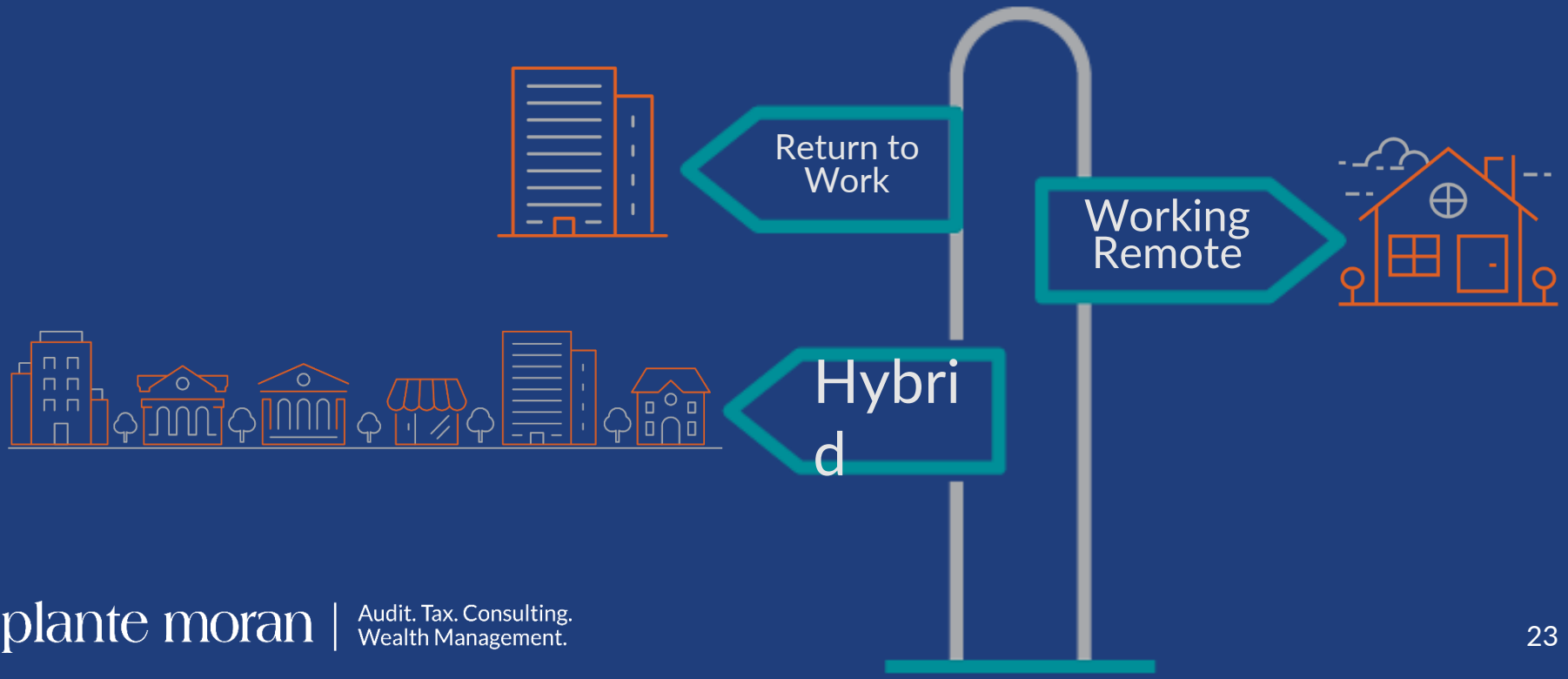
- Effective policies & procedures to protecting firm and client data/systems
- Timely process to patch known vulnerabilities
- How long can you survive without your systems or data? Backup/business continuity
- How will you respond to a Cyber incident? Incident response team and plan
- Proper cyber insurance coverage
- Document retention policies

As threats constantly evolve, your processes to detect and resolve new threats must evolve as well

Technology

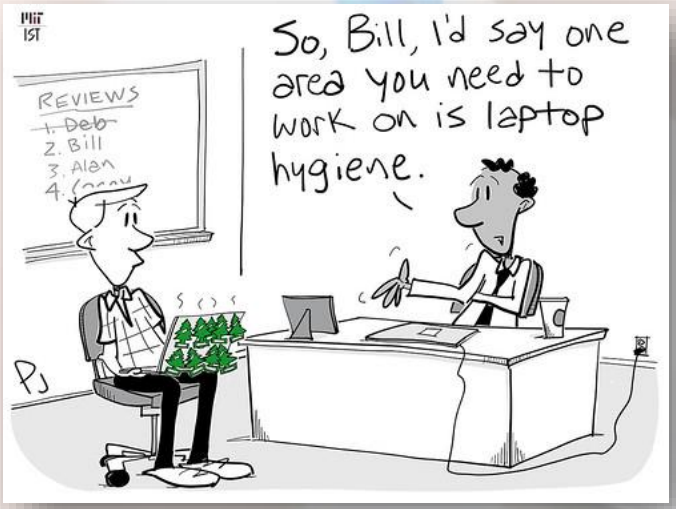

Network & Infrastructure Security
Advanced Threat Protection
NAC
SDN
DDoS Protection
DNS Security
Network Firewall
Deception
ICS + OT
Network Analysis & Forensics
Web Security
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Application Security Testing
MSSP
Traditional MSSP
Advanced MSS & MDR
Data Security
Encryption
DLP
Data Privacy
Other
Mobile Security
Risk & Compliance
Risk Assessment & Visibility
Security Ratings
Pen Testing & Breach Simulation
GRC
Security Awareness & Training
Security Operations & Incident Response
SIEM
Security Incident Response
Security Analytics
Threat Intelligence
IoT
IoT Devices
Automotive
Connected Home
Messaging Security
Identity & Access Management
Authentication
IDaaS
Privileged Management
Identity Governance
Consumer Identity
Digital Risk Management
Security Consulting
Blockchain
Fraud & Transaction Security
Cloud Security
Infrastructure
Container
CASB

Where are we today



“Return to Work”

Devices coming back to your offices



Before devices (laptops, iPads, etc.) can be connected to your network:

- Only corporate laptops are connecting to network
- Devices are up to date on anti-virus
- Scan device for malware
- Scan device for unauthorized software (licensing issue or software with malware)
- Security setting are appropriate (i.e. USB disabled)
- Applications versions are up-to-date
- Backup laptops & devices
- Remember to physically sanitize the devices periodically

Data coming back to your offices

Before data is downloaded to company network or storage locations:

- Complete back of systems and data, before anyone comes to the office
- Scan USB devices for malware before they are allowed to connect to devices
- Scan data from rogue online storage in safe folder (or sand-box) before moved to internal data storage
- Scan email inboxes for rogue attachments/files


Working Remote

Working Remotely

How do employees work seamlessly & securely work from office & home:

- A corporate issued secure device
- Encrypted USB devices
- Encrypted laptops
- Secure online data storage
- Policies for physical safety of corporate devices
- VPN for connecting remotely
- Save sensitive documents in the appropriate/approved locations
- Establish a location to secure sensitive hard copy documents

Working Remotely

How do employees work seamlessly & securely work from office & home:

- Restrict saving passwords in browsers
- Change default passwords for home routers
- Limit the use of public Wi-Fi
- Use a password manager
- Update Operating Systems regularly
- Turn on Authentication for mobile devices

Five cybersecurity considerations

Risk assessment

Have you performed a cybersecurity risk assessment to identify high-risk areas to your organization?

Incident response

Have you had a cybersecurity breach recently? Do you have an incident response plan?

Cyber awareness

Do you have cyber awareness training for employees?

Cyber compliance

Do you receive, store, or process PII, PHI, credit cards, or sensitive data on behalf of your clients or employees?

Return to work

Is your organization prepared for the "new normal?"

Risk assessment

- What are you trying to protect?
- Where is the data stored?
- What are the risks to data & systems? Likelihood & impact?
- What are the controls in place?
- Who is responsible for the data, systems, & controls?

"Risk comes from not knowing what you're doing."

— WARREN BUFFET

Incident response

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery

... most importantly

Lessons learned & communication!

Cyber awareness

All employees — especially C-suite

Important elements

- Annual awareness training
- Phishing tests
  - Consider goals & incentives to get there
- Regular reminders

What is your organization currently doing for cyber awareness?

Cyber compliance

HIPAA • HITRUST • GLBA • PCI DSS • GDPR • CCPA /CPRA • ISO 27001 • SOC

- Understanding applicable standards & regulations
- Reviewing contractual obligations
- Incorporating into risk assessment
- Mapping compliance requirements | “Test once, apply to many.”
- Educating IT department on compliance

Return to work

What are some key cybersecurity considerations?

Key cyber takeaways

Risk assessment

Use your risk assessment to make sure your cybersecurity resources are being used wisely.

Incident response

It's not "if", but "when."
Be prepared.

Cyber awareness

Give your people the tools they need to be cyber awareness gurus.

Cyber compliance

Make sure you know what you need to be compliant with.

Return to work

Don't let cybersecurity be an afterthought when designing what your "new normal" will look like.


Q&A

Contact your presenters

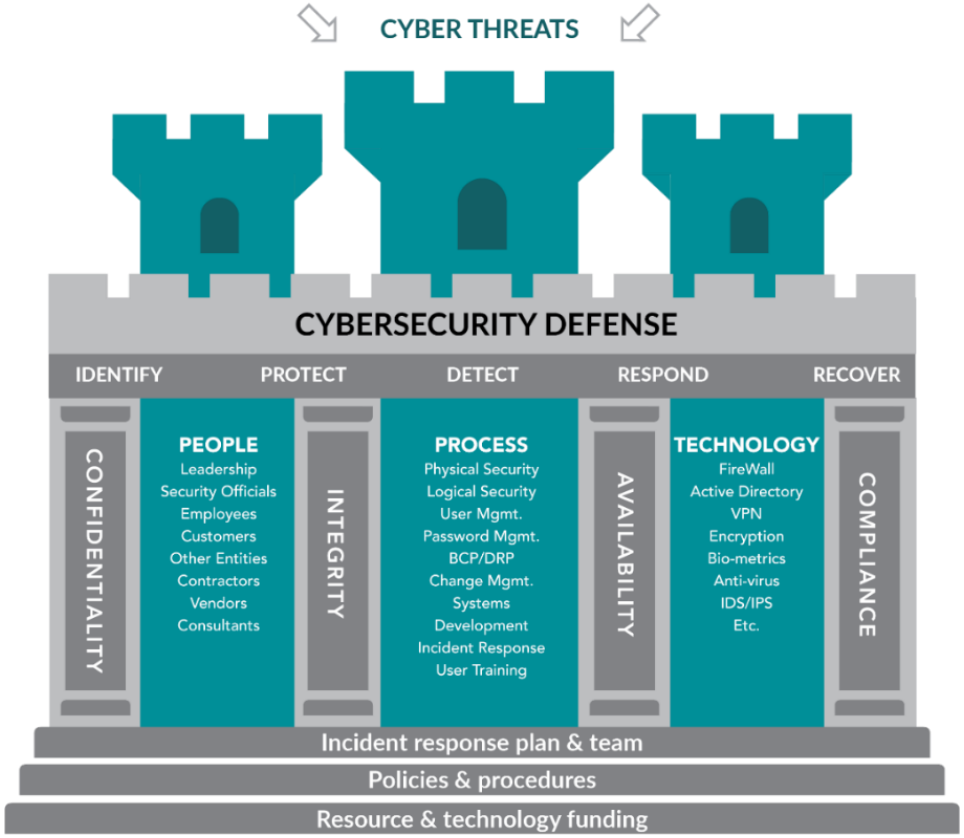
Furney Brown
Principal, MC-Cybersecurity
248-223-3396
Furney.Brown@plantemoran.com

Jen Fiebelkorn
Principal, MC-Cybersecurity
248-223-3365
Jennifer.Fiebelkorn@plantemoran.com

How we can help

Cybersecurity

Fortify your cybersecurity defenses with people, processes, and technology



Cybersecurity Services

As cyberattacks grow more sophisticated, complex, and financially devastating, organizations still struggle to mitigate security breaches. Plante Moran has developed the following consulting services to help organizations:

Cyber governance

Do you fully understand the NIST cybersecurity standards or the SANS Top 20 security controls? Are you confident in the integrity of your information? We'll help you develop a risk governance framework and a cybersecurity roadmap that's manageable and sustainable for your organization and culture.

IT audits

Auditing your IT and cyber controls isn't merely a prudent measure; it's required in regulated industries. An audit can identify gaps and expose issues with the controls in your current security systems, allowing you to address them before a cybercriminal takes advantage of your systems' weaknesses.

Security compliance

Are you prepared to comply with various privacy regulations (GLBA, HIPAA, GDPR, etc.) and industry standards (such as PCI DSS, HITRUST, ISO 27001)? We'll map your control environment against each applicable requirement and provide a concise overview of your compliance status dashboards.

Cyber risk assessments

We'll guide you through a cyber risk assessment methodology that identifies and addresses the specific threats your organization faces. This eye-opening exercise is critical; without it, you simply can't know if you have the correct controls to mitigate the perceived risks.

SOC examinations

Our services include the newly released SOC for cybersecurity. We also perform more than 50 SOC 1, SOC 2, and SOC 3 examinations annually with clients across the United States and globally. We'll perform readiness assessments to identify control weaknesses and develop recommendations for remediation.

Attack & pen testing

Using the most current threat intelligence, our cybersecurity specialists work with you to identify specific target areas and launch controlled cyber attacks from common footholds to identify gaps and weaknesses.