It's a New Cyberworld.

October 26, 2021

Norman Comstock, Managing Director

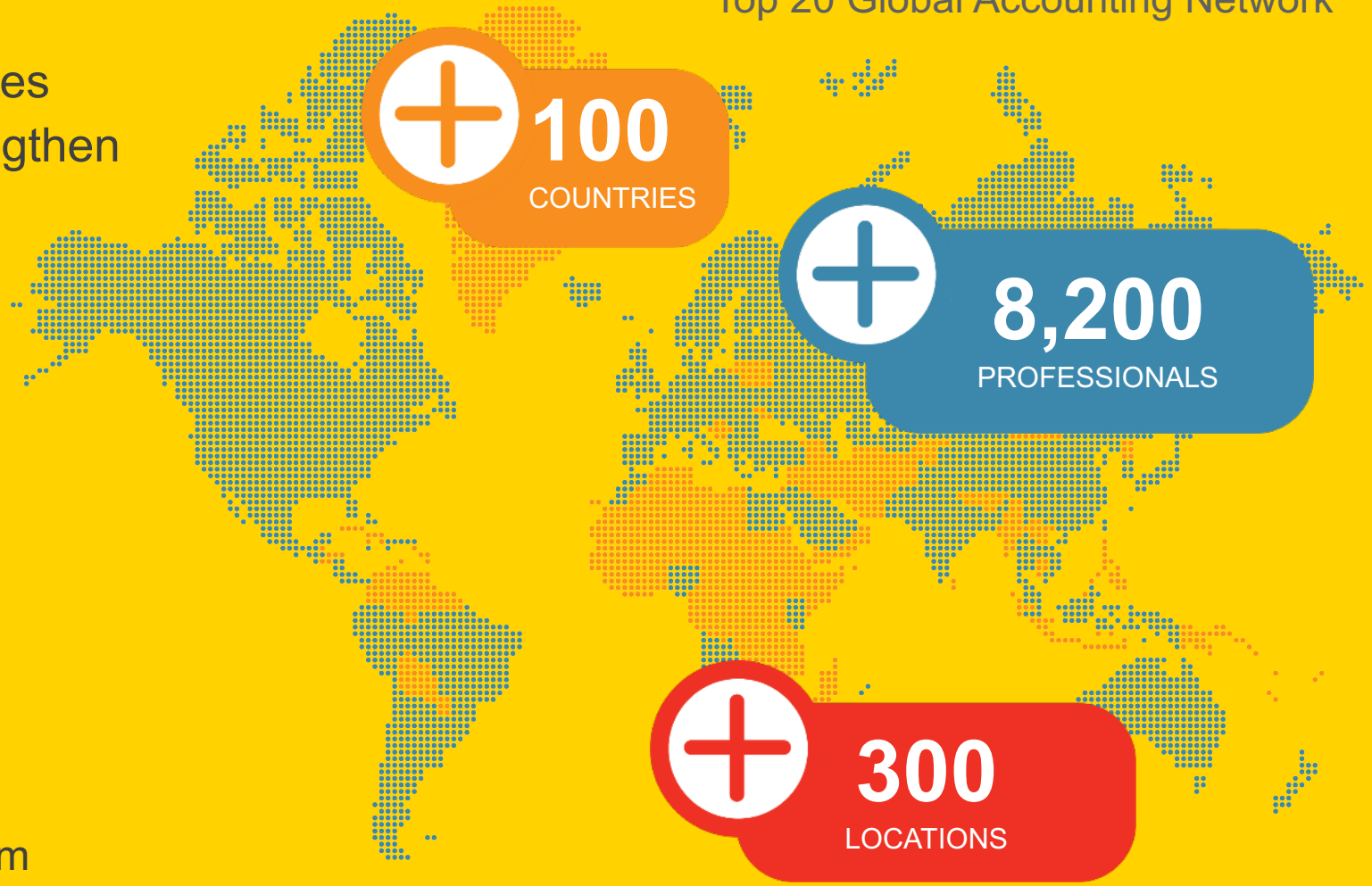
Norman Comstock, Managing Director Cybersecurity, UHY Consulting

Lecturer since 2006	**University of Houston's C.T. Bauer School of Business**
Professional Association Memberships	IIA Houston, ISSA South Texas, ISACA Greater Houston Chapters
Focus	IT Governance and Cybersecurity risk
MBA and MS International Business	Cameron School of Business University of St. Thomas
BBA in Accounting	University **of Houston**

"Married my beautiful bride over 30 years ago; Proud father of two young men that have recently graduated from college; Enjoy golf, tennis, saltwater fishing and BBQ."

Member of UHY International
Top 20 Global Accounting Network

UHY Consulting is a management consulting firm that guides companies through **transformations** that strengthen organizations.



Our key capabilities:

- Business and Strategy
- Organization and Operations
- Finance and Accounting
- Business Applications
- Technology Innovation
- Cybersecurity
- Resource Solutions

Affiliate of UHY LLP
A national certified public accounting firm

Our Agenda Today

An Overview of Cybersecurity

6 Cyber Savvy Questions

Q&A

Cybersecurity is not an option.

Hackers are motivated and well-funded

Expanding Attack Surface

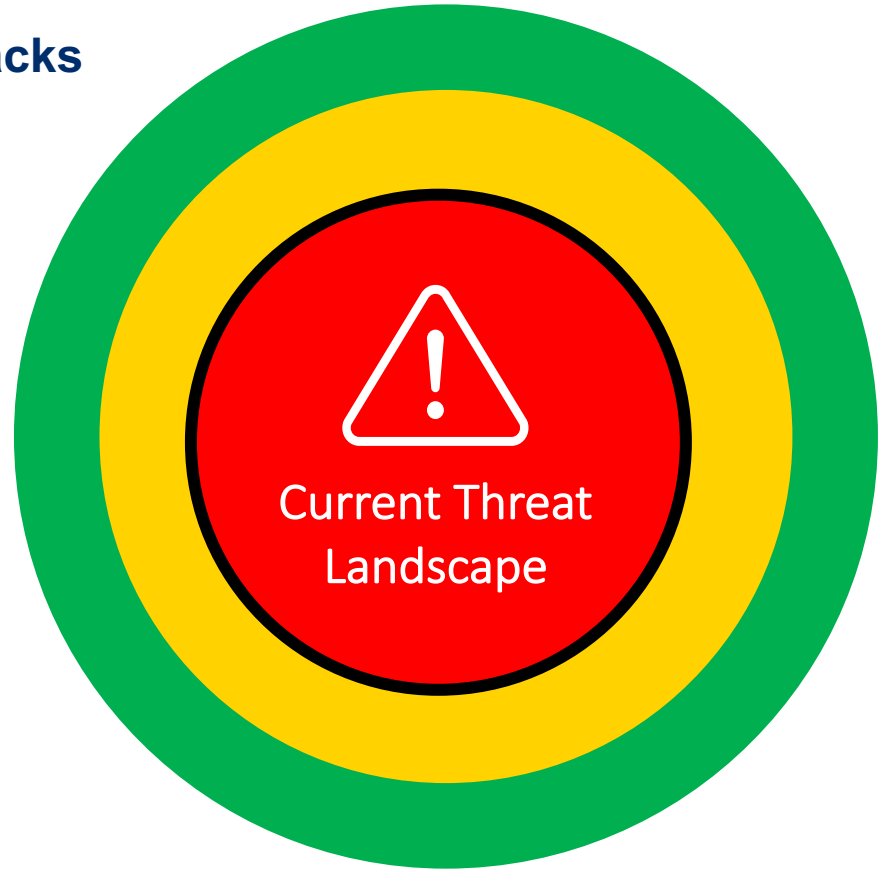
- Endpoint
- Network
- Cloud and SaaS
- Users
- IoT
- Mobile Devices

Motivated and Well-Funded Threat Actors

- Malicious Insiders
- Terrorists
- Organized Crime
- Hacktivists
- Nation States

Creative and Sophisticated Attacks

- Spear-Phishing
- Custom Malware
- Zero-Day Exploits
- Social Engineering
- Physical Compromise



Hackers are motivated and well-funded

Well-Established Cyber-Crime Economy

50¢ to $20
Credit Card Number, Email Accounts (per 1000)

$7 to $8
Cloud Accounts

Up to $50
per Healthcare Record

Up to $3,500
Custom Malware

Up to $1,000/day
DDoS Attack

The Current Situation

Increase in cyberattacks

154% increase in cyberattacks in first 6 months of 2020 over 2019

Malware by email

92% of malware is delivered by email

Phishing emails

97% of people globally are unable to identify a sophisticated phishing email

Spear phishing

95% of attacks on business networks result from successful spear phishing

Business Email scams

$26 Billion lost to Business email compromise (BEC) scams from 2016 to 2019

$1.6 million and rising

The average cost of a phishing attack to a mid-size company is……. $1.6 Million & Rising!

Source: FBI Internet Crime Complaint Center, Ponemon Institute, Verizon DBIR

It’s time to plan for a rainy day.

6 QUESTIONS to ask your IT Department

1.) Do we have a robust incident response capability in place?

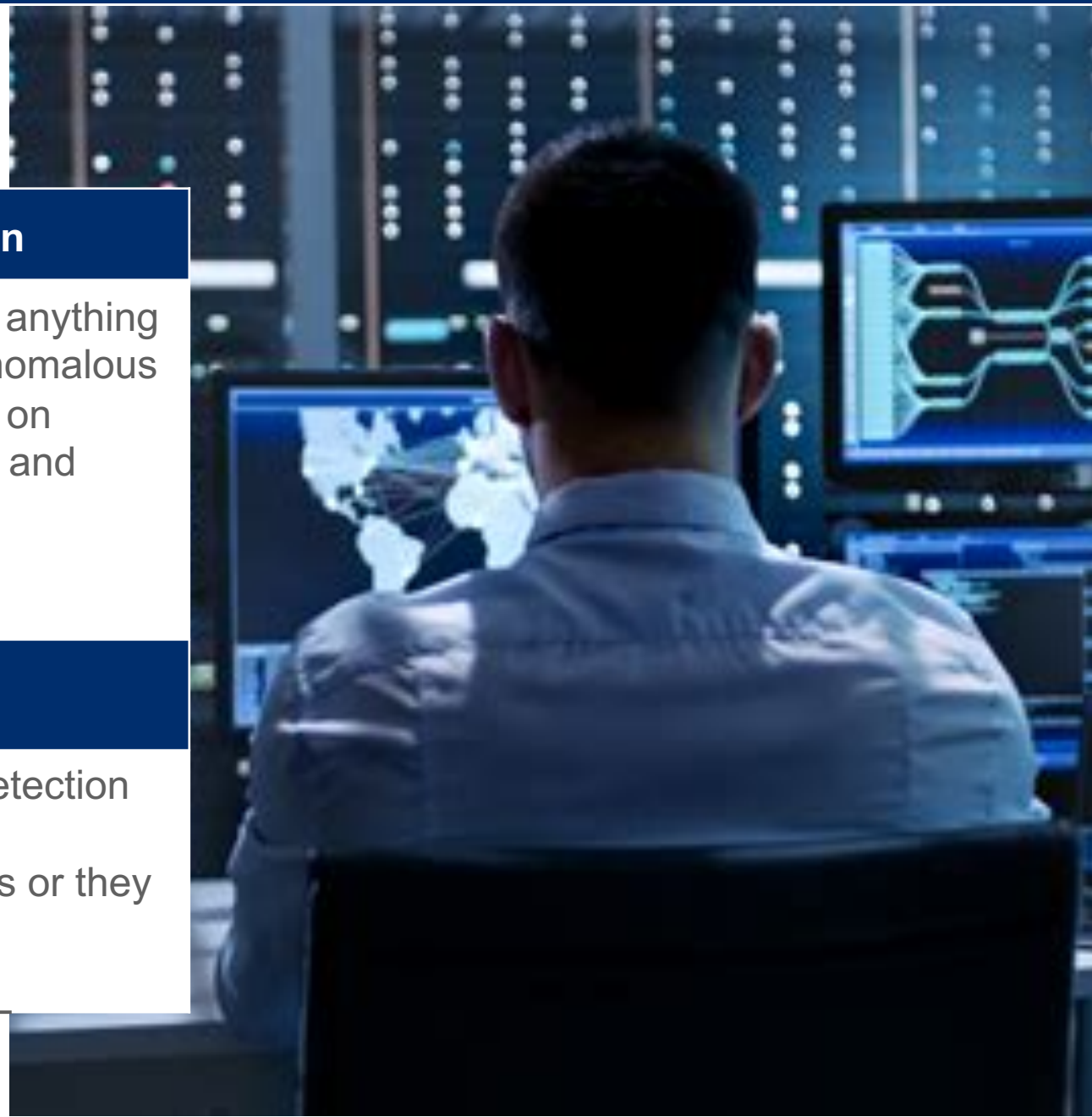
UHY Consulting

Incident response capability

What You Want to Hear	Warning Sign
Yes, we have software that provides alerts and possibly a third-party provider to help monitor our system around the clock and responds through quarantine or other isolation capabilities.	No, we do NOT have anything in place to monitor anomalous or known bad activity on servers, workstations and laptops at all hours

What can Companies do?

- Consider deploying a next generation, endpoint detection and response security tools.
- Determine if IT can respond to the identified issues or they need outside assistance



6 QUESTIONS to ask your IT Department

“2.) Do we have a regular program to scan our network and applications for vulnerabilities?”

UHY Consulting

Scan our network?

What You Want to Hear	Warning Sign
Yes, our company has a regular program to scan our network, applications, web services, and networked devices inside and from the internet in place	No, we do NOT regularly scan our network, software applications and device configurations.

What can Companies do?

- Ask IT to conduct a vulnerability scan as soon as they can to begin to identify and patch or remediate any high risk and critical vulnerabilities
- At a minimum this should be done quarterly on internal assets and from an internet perspective

6 QUESTIONS to ask your IT Department

3.) Do we have good backups of critical systems, date and configurations?

UHY Consulting

Data Back Ups?

What You Want to Hear	Warning Sign
Yes, in case of a cyber event, our company has… • Backups of critical systems, data and configurations • Tested • Stored offsite or in the cloud	No, we do NOT have the ability to successfully restore operations from a backup and/or back-up files are onsite

What can Companies do?

Work to minimize business continuity risk with your important systems:

- Confirm that all IT systems are included within the backup solution
- Ensure that they are tested periodically
- Treat backup files as critical data and isolated from the rest of the network
- Ensure a full copy of the backups is stored offsite

6 QUESTIONS to ask your IT Department

4.) Do we have an incident response plan for a cyber-attack?

UHY Consulting

Incident Response?

What You Want to Hear	Warning Sign
Yes, our company has a solid plan in place… • Regularly tested • Employees understand their roles depending on the situation	No, there is NO cyber-attack or overall incident response plan

What can Companies do?

- Identify who to contact if a cyber incident is happening.
- Document the expected actions to be performed in the event of an incident
- Perform tabletop tests of the plan before a real event occurs.
- Establish a cyber 911 call service that will quickly focus response activities to stabilize the environment and begin the recovery process

6 QUESTIONS to ask your IT Department

5.) Do we have an employee security awareness program?

UHY Consulting

Security Awareness?

What You Want to Hear	Warning Sign
Yes, our employees are our best source of defense… • We have a continuous testing program in place • Staff stays alert and vigilant	No, our employees do NOT understand the extreme threat that phishing emails can pose to our company

What can Companies do?

- Phishing emails remain the easiest and most likely way to get into your business to steal data, access your internal network or begin the staging of malicious software
- IT or an outside vendor can build an internal program to regularly phish employees

6 QUESTIONS to ask your IT Department

6.) Do we have cyber insurance?

UHY Consulting

Cyber Insurance?

What You Want to Hear	Warning Sign
Yes, we have a cyber insurance policy… • Clearly outlines what the policy does and does not cover • We understand the carrier's role versus our role • Understand operational risks not covered by insurance	No, we do NOT have a cyber-attack or overall incident response plan that includes cyber insurance

What can Companies do?

- Don't put your company's brand, your clients' trust and your future at risk
- An insurance broker can provide guidance on a policy and help you manage your risk appetite for a cyber loss
- Ask specific questions on what losses are covered, including such things as public relations, ransomware payments, incident responders and digital forensics

Stay balanced in this new Cyberworld!

Important Take-aways!

- Locks can/will be broken

- Planning and vigilance is necessary

- Don’t spin your wheels; Ask your questions and seek advice for your specific situation

Questions

Norman Comstock
ncomstock@uhy-us.com