Cybersecurity Myths Debunked

January 27, 2021

WINDES

AUDIT | TAX | ADVISORY

ALLIANT

CYBERSECURITY

WINDES OVERVIEW

- Established in 1926
- 29 Partners, 180 Total
- Audit & Assurance Services
- Tax Services
- Advisory Services
  - Cybersecurity
  - Employee Benefit Services
  - Mergers and Acquisitions
  - Outsourced Accounting Services
  - Paycheck Protection Program (PPP) Loan Forgiveness
  - Value Acceleration and Exit Planning
- Full-Service Offices in Long Beach and Irvine
- Satellite Office in Los Angeles
- 5,000+ Clients
- Diversified Across all Industries with the Exception of Banking
- National and International Network Through Baker Tilly International

ALLIANT CYBERSECURITY OVERVIEW

ALLIANT CYBERSECURITY
An alliantgroup Company

Alliant Cybersecurity was founded by industry leaders with decades of experience in enterprise risk management, cybersecurity, professional services and legislation.

We work with leadership within professional services firms and their clients to implement security strategies, offer advisory services and comprehensive policies and procedures tailored to the unique needs of the middle market.

Presenters

Rebecca Christiansen, CPA, MST

Windes Director of Operations & Information Technology

562.304.1320

rchristiansen@windes.com

Jon Murphy

Alliant Cybersecurity Consulting Practice Lead & Vice President

832.388.4004

Jon.Murphy@alliantcybersecurity.com

Rebecca Christiansen – Windes

Rebecca joined Windes in 2005 as a staff accountant in the Tax department, after graduating from the University of California, Los Angeles. Over the next 5 years she worked in client service and in 2011, Rebecca left the tax practice to join the firm's administration as Manager of Operations. Over the next 10 years, her role evolved to include overseeing the firm's IT and cybersecurity. In 2017, Rebecca was named Director of Operations/Information Technology.

Rebecca Christiansen, *Windes Director of Operations and Information Technology*

Originally focused on the direction and coordination of the firm's internal activities, such as personnel training, facilities management, IT and cybersecurity, Rebecca returned to client service with the launch of Windes Cybersecurity. This practice offers a full suite of cybersecurity services including cyber risk assessments, vulnerability assessments, penetration tests, and incident response and preparedness. Through a partnership with a team of cybersecurity experts, Windes is also able to offer managed security services, framework assessments, security training, cybersecurity compliance consulting, and audits. Rebecca conducts numerous trainings on a variety of technical and professional topics and writes a regular cybersecurity blog for the firm's website.

JON MURPHY– ALLIANT

Jon has 25+ years of success as a Business Technology Leader and IT Risk Management Consultant. He has created and led Technology Risk Management programs for federal and state governmental entities, eCommerce organizations, and many other verticals. Jon has delivered effective leadership in privacy by design, advanced cybersecurity, organizational resiliency, and governance-risk-compliance (GRC) programs across dynamic environments.

Expertise

- Strategic business planning
- Business Process and Technology integration
- Cloud Security
- DevSecOps/Application Security
- P&L Management
- Disaster Recovery and Business Continuity Planning
- Remediation and Road-map planning

Experience

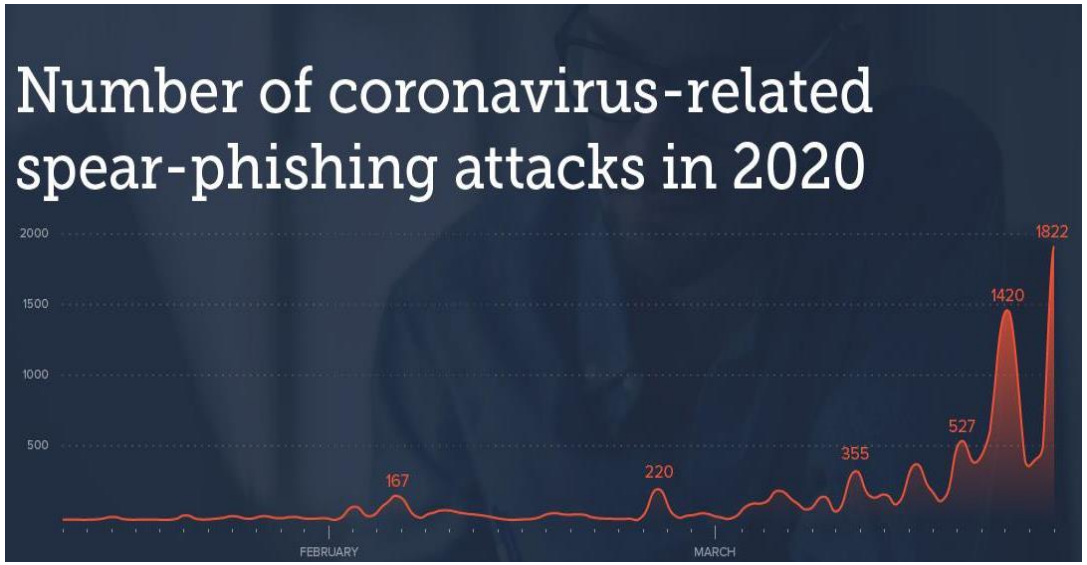
- Experience of 25+ years in Information Technology and operational risk management
- Integrated people, process, and technology to drive implementation of a cohesive strategy for globally complex and diverse enterprises
- Provide thought leadership across cybersecurity domains and assures seamless integration of enterprise security and risk frameworks
- Internationally published articles and discussions on cybersecurity and data privacy related subjects on various platforms and forums
- Created and delivered customized, innovative solutions for many clients and industries.
- Co-authored the current physical and logical model for all National Special Security Events (NSSE); employed at events like super bowls, inaugurations, and world cups.

Please submit questions
using the Q&A button
at the bottom of your screen.

Cybersecurity in the time of COVID

CYBERSECURITY IN THE TIME OF COVID

- The FBI reported that the number of complaints about cyberattacks to their Cyber Division is up to as much as 4,000 a day, a 400% increase over pre-coronavirus.
- Zohar Pinhasi, a cyber counter-terrorism expert, reports that ransomware attacks are up 800% during the pandemic.
- Only 41% of cybersecurity professionals say their companies are utilizing best practices to secure a remote workforce.



CYBERSECURITY IN THE TIME OF COVID

"This is a once-in-a-lifetime target-rich environment for fraudsters. The number of people that are potential targets, that could be easily duped by sophisticated cons, is the greatest I've ever seen in my life."

-Thomas C. Edwards
Special Agent in Charge
San Francisco Office
U.S. Secret Service

THE THREAT LANDSCAPE

FOUR DIFFERENT AREAS OF THREAT ACTORS

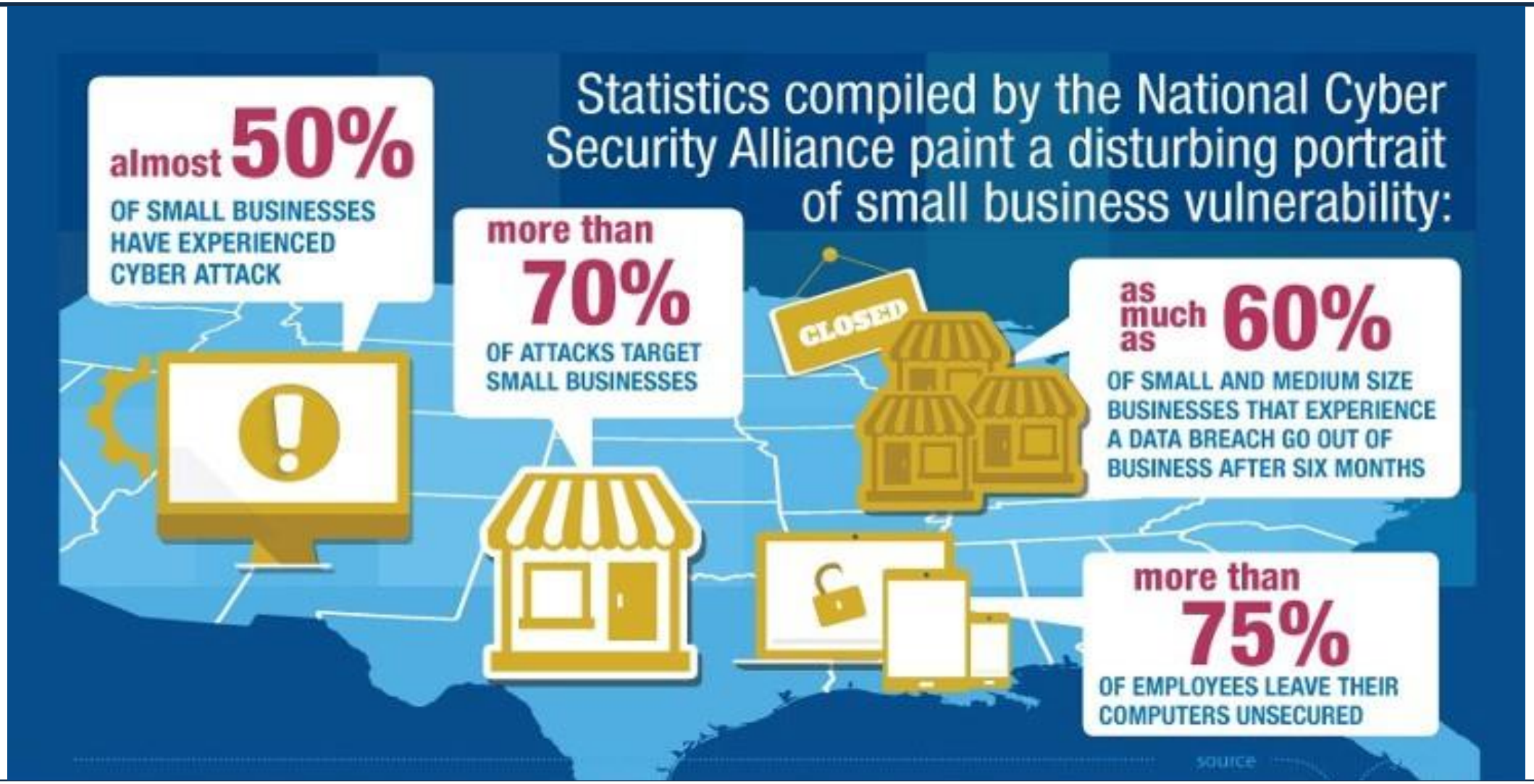
Cyber Criminals

Insider Threats

Hacktivists

Nation States

More Bad News



CONSIDER…

- 500,000 cyber attacks – PER MINUTE
- Cyber crime pays bigtime because organizations are neglecting the fundamentals
- Every 14 seconds an organization will be hit with ransomware
- 50% of organizations that pay ransom, will not get their data back
- 50% of those that do get it back, get hit with another form of attack (ransomware, cryptomining, DDoS, etc.) within 90 days

Top 7 Cyber Myths

#1 Cyber Myth

1. My internal IT team or an external Managed Service Provider is taking care of my cybersecurity…

INFORMATION TECHNOLOGY vs. CYBERSECURITY

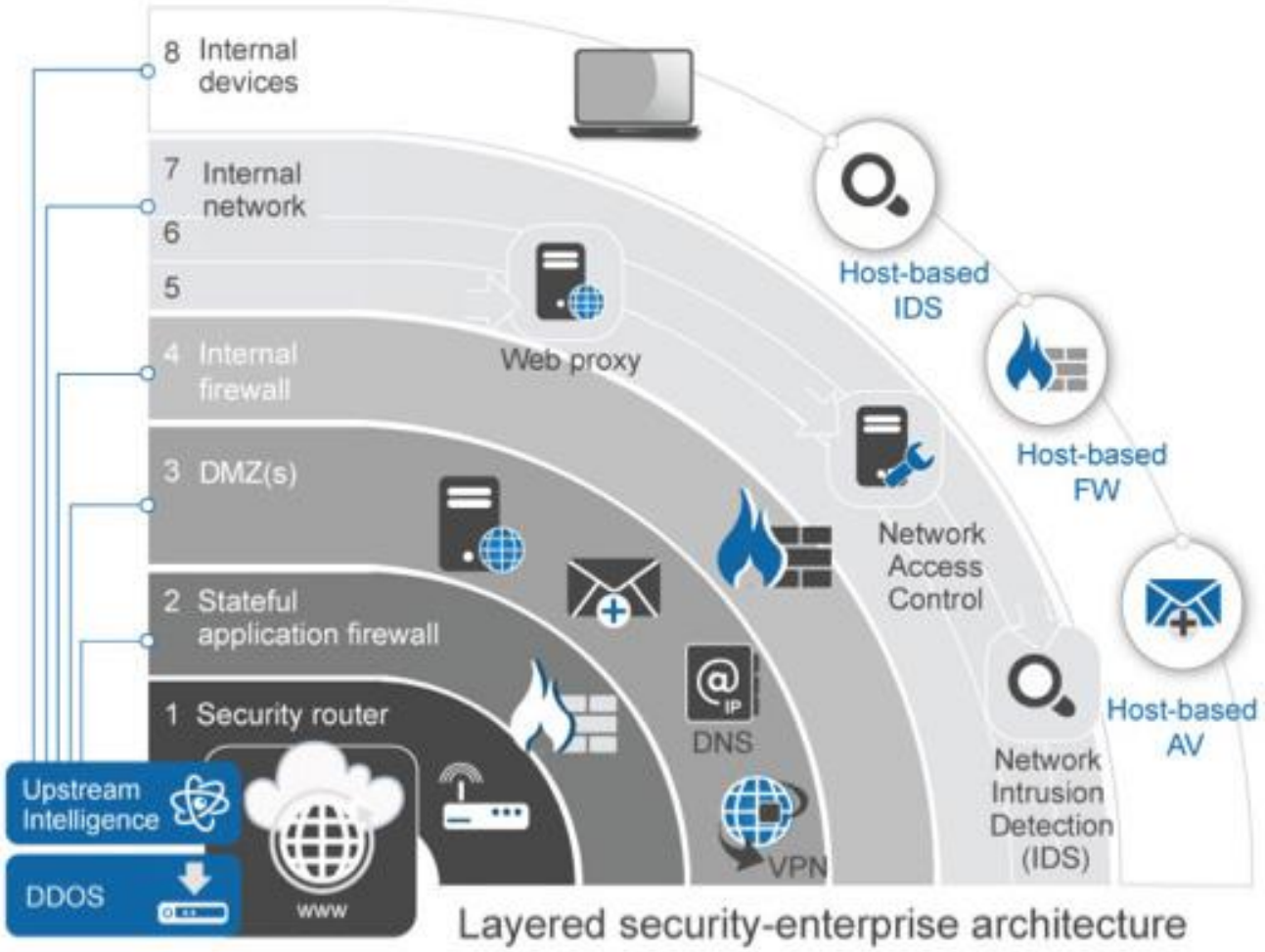
What is the difference and why do we need both?

	Information Technology	Cybersecurity
	Top priority: **Ensuring** hardware, software, and other network components remain functional	Top priority: **Protecting** data and assets
	Responsible for **hardware, software, and new technology**	Responsible for **systems, processes, and risks** posed by end users
	**Puts** controls in place	**Monitors** controls to ensure they work as intended
	Stays up-to-date on new **hardware, software, and solutions**	Stays up-to-date on new **threats and developments** that emerge daily
	Often measured in **uptime and response time**	Recommends and **prioritizes action** steps and solutions
	**"Fix-it"** mentality	**"Secure-it"** mentality

#2 Cyber Myth

2. OK, but we have anti-malware and a good firewall so that technology has it all covered.

Defense in Depth



Takes layers of integrated technology that is tended to by experts

#3 Cyber Myth

3. We are covered if any cybersecurity incident happens because we have a Cyber Liability Insurance Policy.

Cyber Liability Insurance Policies

- Many insurance companies have started to withhold funds because the insured is not following cyber best practices.
- The loss of customer reputation in the highly sensitive CPA field can be devastating, even if the costs are fully covered by the policy.
- The Treasury Department is proposing levying fines for businesses & insurance companies that actually pay ransoms

#4 Cyber Myth

4. Phishing scams are easy to spot.

YOUR PEOPLE ARE BUSY

- Phishing scams are becoming more sophisticated as hackers infiltrate companies, CEO's personal accounts (Business Email Compromise -BEC),
and even government agencies.

- Even smart, loyal professionals fall victim; one wrong click is all it takes.

- Phishing scams are up nearly 50% since COVID-19 lockdowns, targeted teleworkers.

- Deepfakes increasing too

#5 Cyber Myth

5. We have data backups so if we get infected with ransomware we will just restore from our backups.

ARE YOU *SURE* YOU HAVE BACKUPS?

New ransomware variants can readily jump to online, local backups, so . . .

- Backups should be in a 3-2-1 strategy
- Backups should be routinely performed on a schedule
- Backups should be encrypted, but ideally, without *breadcrumbs*
- Backups should routinely be test restored

#6 Cyber Myth

6. I’d know right away if something bad was in my computer or network.

Dwell Time & Operational Insight

- Bad Actors often gain access and then do nothing, learning about your organization for months, before launching their attack
- What tools do you have or does your IT shop have that would alert you to such a stealthy approach?
- Takes full time, “eyes on glass”, artificial intelligence, and deep learning technology
- A Managed Detection and Response Service is an excellent way of addressing dwell time

#7 Cyber Myth

7. My network is in the cloud, so my cloud provider is handling security.

CLOUD SECURITY IS STILL *YOUR* RESPONSIBILITY

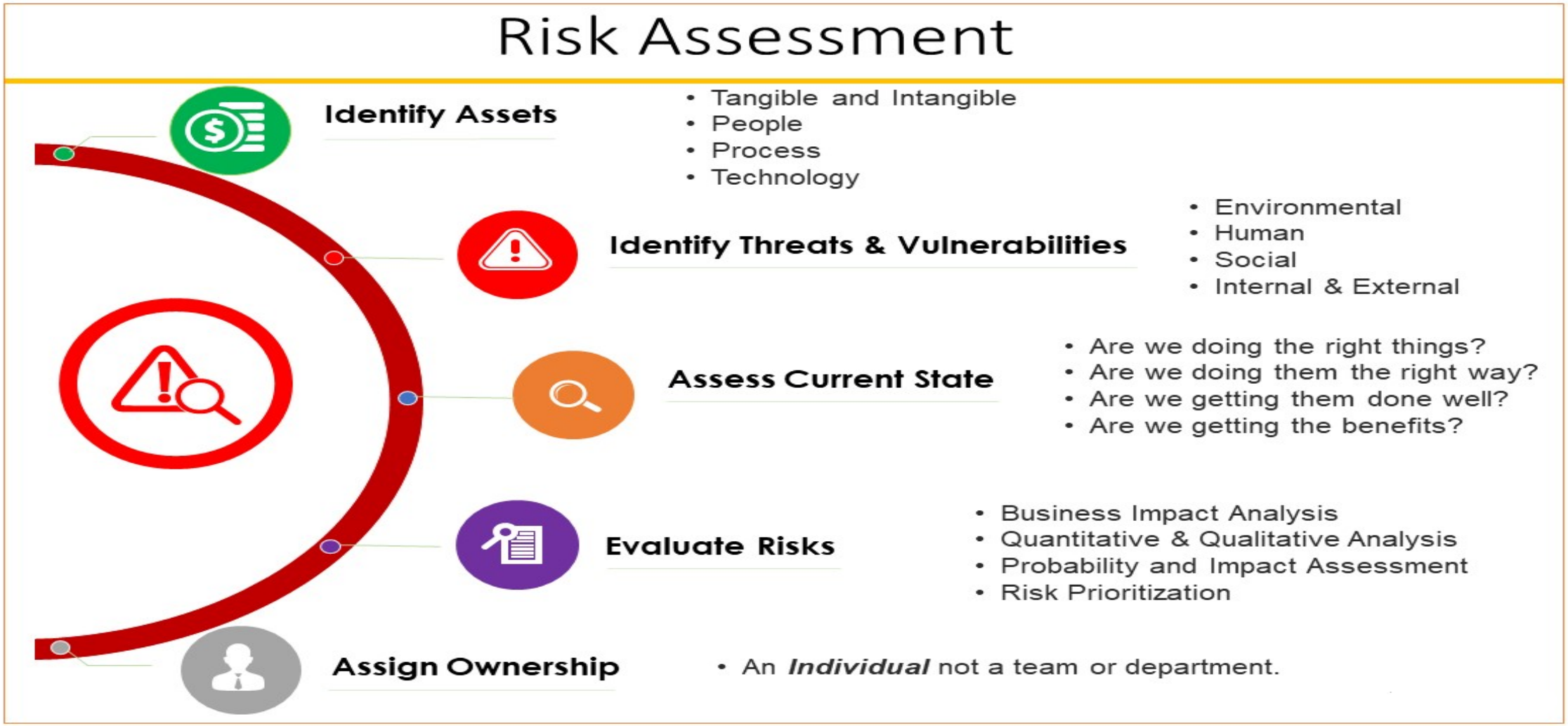
Security *of* the Cloud is provided by the Cloud Services Provider (CSP – Amazon, IBM, Azure, etc.)

Security ***IN*** the Cloud is YOURs. That includes

- Configuration Management
- Systems and Data Access Controls
- Applications Patching
- Backups
- Encryption, etc.

What Can You Do?

1 – Perform a Risk Assessment

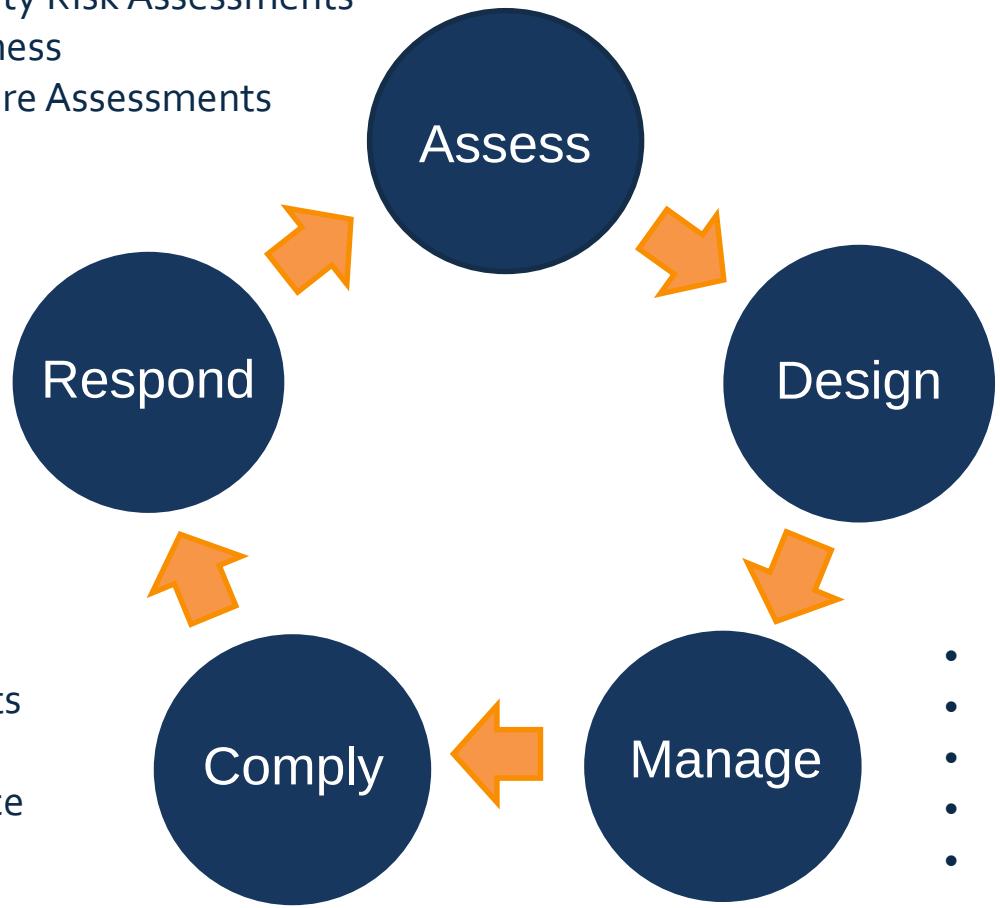


Next Steps – Building a Roadmap

1. **Review your corporation's formal risk appetite statement for cyber issues, if you have one – otherwise create one**
2. **Determine how your organization rates and ranks within your industry**
3. **Have a dialogue with your IT/MSP on what the state of their cybersecurity is**
4. **Determine next steps in a risk ranked, prioritized approach to make adjustments accordingly**
5. **Continual education and training of staff**

Understand that Cybersecurity is a Journey

- Cybersecurity Risk Assessments
- SOC Readiness
- Infrastructure Assessments



- Network Security
- Data Protection
- Infrastructure Design
- Cloud Security
- Technology Consulting

- Incident Response Planning
- Business Continuity and Disaster Recovery
- Digital Forensics

- Framework Assessments
- Data Privacy
- Government Compliance
- Compliance Readiness

- Education and Awareness Training
- Policy Planning
- Penetration Testing
- Virtual CISO
- Managed Security Services

Free Informational Resources

How secure is your password

https://lastpass.com/howsecure.php

An article on BEC – Business Email/Process Compromise

https://alliantcybersecurity.com/business-email-compromise-bec-what-you-need-to-know//

Has your email been compromised

https://haveibeenpwned.com/

An Article on What Courts say is a “Reasonable” Cybersecurity Posture

https://alliantcybersecurity.com/cybersecurity-risk-what-does-a-reasonable-posture-entail-and-who-says-so/

Questions?