CYBERSECURITY DOESN'T HAVE TO BE SCARY:

Protecting Your Growing Business

rea BUSINESS ADVISORS

Jeff Rapp
Principal
Jeff.Rapp@reamanaged.com

Travis Strong
Principal
Travis.Strong@reamanaged.com

Steve Grossenbaugh
Business Development Manager
Steve.Grossenbaugh@reamanaged.com

rea BUSINESS ADVISORS

Agenda

Setting the Stage: What's happening on Elm Street!?!	Ward Off Cyber Goblins & Banish Security Ghosts	Survive Compliance Scares	Web of Protection – Layered, Scalable Security	Escape the IT Nightmare – Organizational Strategy
				
We will discuss why cybersecurity matters for organizations, including the realities of the situation and some of the most common threats.	We will walk through example attacks and give you the outline of the minimum necessary security protections you should have in place for them.	Compliance matters can be overwhelming and confusing. Here we'll talk about some of the common regulations and how to align your efforts.	Here is your cheat code for protecting your organization. We'll talk about defense in depth, combining multiple layers of security.	Where do I start and how do I get there? These questions are answered to help you build a security culture, balances operations with security.

rea BUSINESS ADVISORS

Poll # 1

If your organization was in a horror movie, what would be the biggest cyber villain?

rea BUSINESS ADVISORS

What's happening on Elm Street?

rea BUSINESS ADVISORS

The realities

🏢 Cyber risk isn't just an IT issue

🔐 Cybersecurity doesn't have to be intimidating

📈 Threats are growing

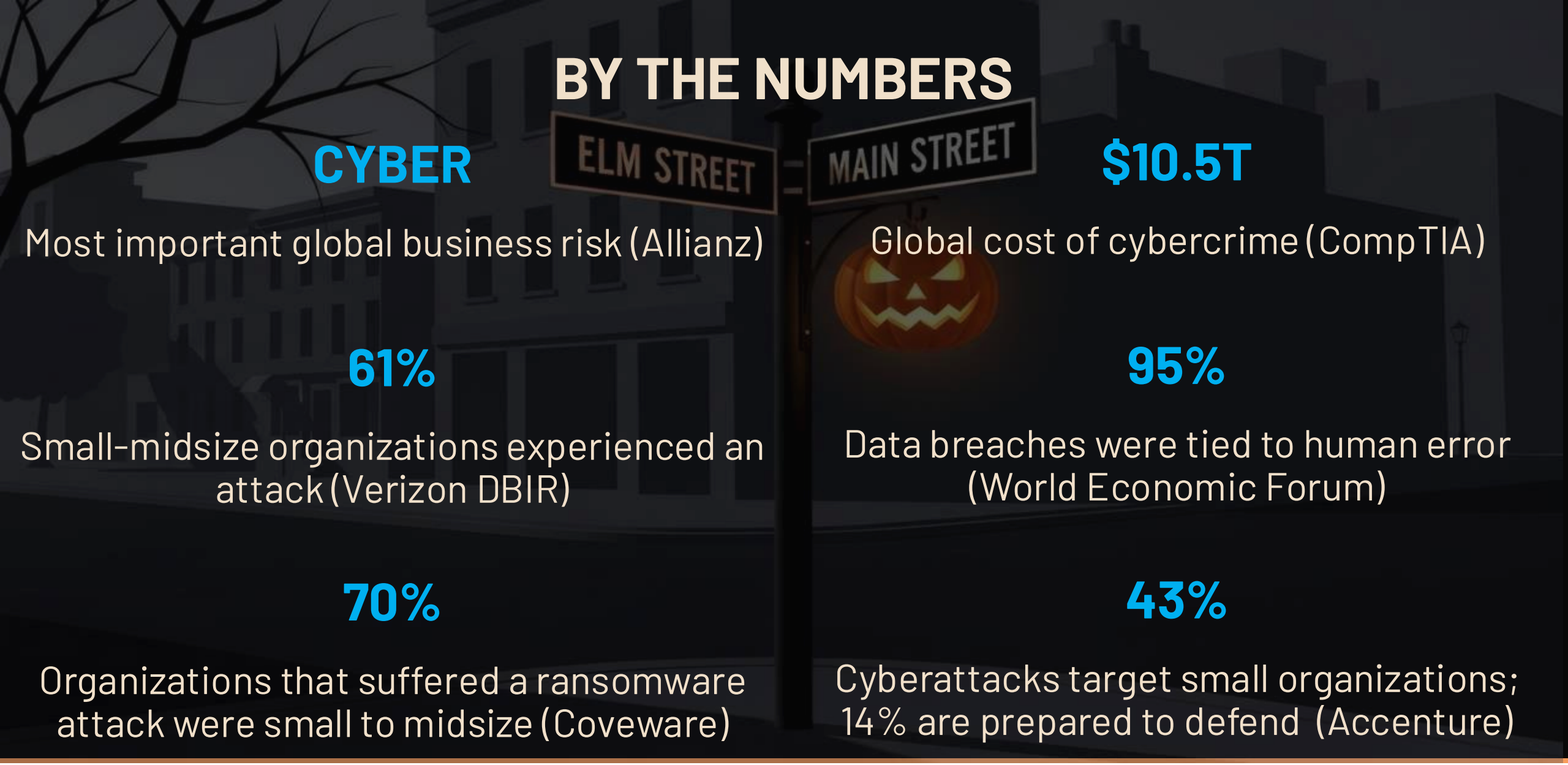
🎲 Many attacks are opportunistic

🤖 Cybercrime is more automated & organized

🌐 No industry is immune to the threats

🎯 Small - midsize organizations are prime targets

rea BUSINESS ADVISORS



BY THE NUMBERS

CYBER

Most important global business risk (Allianz)

$10.5T

Global cost of cybercrime (CompTIA)

61%

Small-midsize organizations experienced an attack (Verizon DBIR)

95%

Data breaches were tied to human error (World Economic Forum)

70%

Organizations that suffered a ransomware attack were small to midsize (Coveware)

43%

Cyberattacks target small organizations; 14% are prepared to defend (Accenture)

rea BUSINESS ADVISORS

THE THREAT LANDSCAPE

Phishing & social engineering

- Phishing remains a leading attack vector
- Attackers use social engineering to trick users
- AI makes it easier (or more difficult)

Ransomware & extortion

- Remains one of the most prevalent threats
- Double-extortion tactics
- Outdated systems, weak passwords, flat networks

Insider threats

- Malicious or accidental actions; manipulation
- Individuals may leak or misuse sensitive data
- Excessive/outdated permissions; onboarding/offboarding

3rd parties, cloud & supply chain security

- Reliance on 3rd parties expands the threat landscape
- Attack surface expands beyond your four walls
- Cloud misconfigurations open up risks

Legacy systems

- Outdated / vulnerable systems are low-hanging fruit
- Difficulty patching/updating leaves them exposed

rea BUSINESS ADVISORS

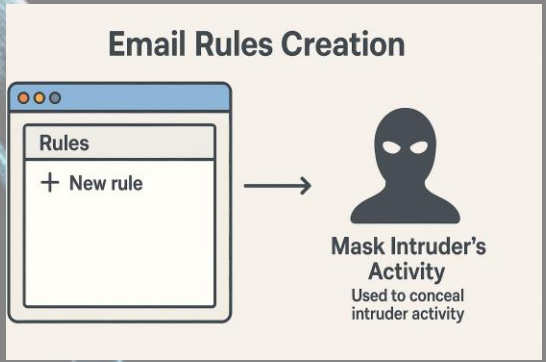
Cyber threats are real, but **they're not unbeatable**. What matters is **visibility, basic controls, and a clear plan**. The rest of today's session will show you how to do just that — without overcomplicating it.

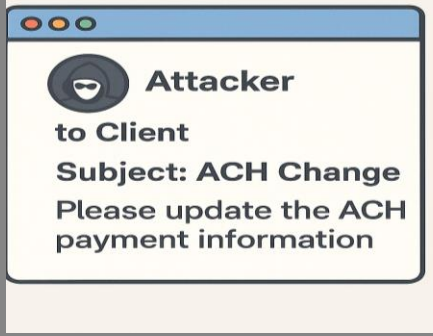
rea BUSINESS ADVISORS

Ward Off Cyber Goblins & Banish Security Ghosts

rea BUSINESS ADVISORS

Business E-mail Compromise (BEC)





Proper e-mail security setup (DKIM, SPF, DMARC)

E-mail Security with link and attachment protection

End user security awareness testing

Licensing that prevents MFA Token hijacking

End user security awareness training

Alerting on risky user logins and abnormal behavior

Alerts for mail flow or mailbox rule creation

Incident Response Plan

Documented ACH Change Rules

rea BUSINESS ADVISORS

Data Exfiltration and Ransomware

Remote connection
Using compromised credentials

Compromise admin accounts and vulnerabilities

Investigate and spread across network

Data Exfiltration

Initiate Ransomware

rea BUSINESS ADVISORS

Data Exfiltration & Ransomware Protections

Internet Security

Business Class Firewall

MFA on VPN and Remote Access

24x7 Monitoring of connections and file transfers

User Security

Security Training and Testing

Audit accounts and permissions

No local and domain admin rights

Limit qty of admin accounts

Endpoint Security

Next Gen Endpoint Detection (AV)

Continuous vulnerability mgmt

24x7 Security and Log Monitoring

Regular patching for OS and Apps

Disaster Planning

Regular Backups w/offsite storage

Annual restore testing

Incident Response Plan

Disaster Recovery Plan

rea BUSINESS ADVISORS

Poll # 2

Will you survive the night?

rea BUSINESS ADVISORS

Survive compliance scares

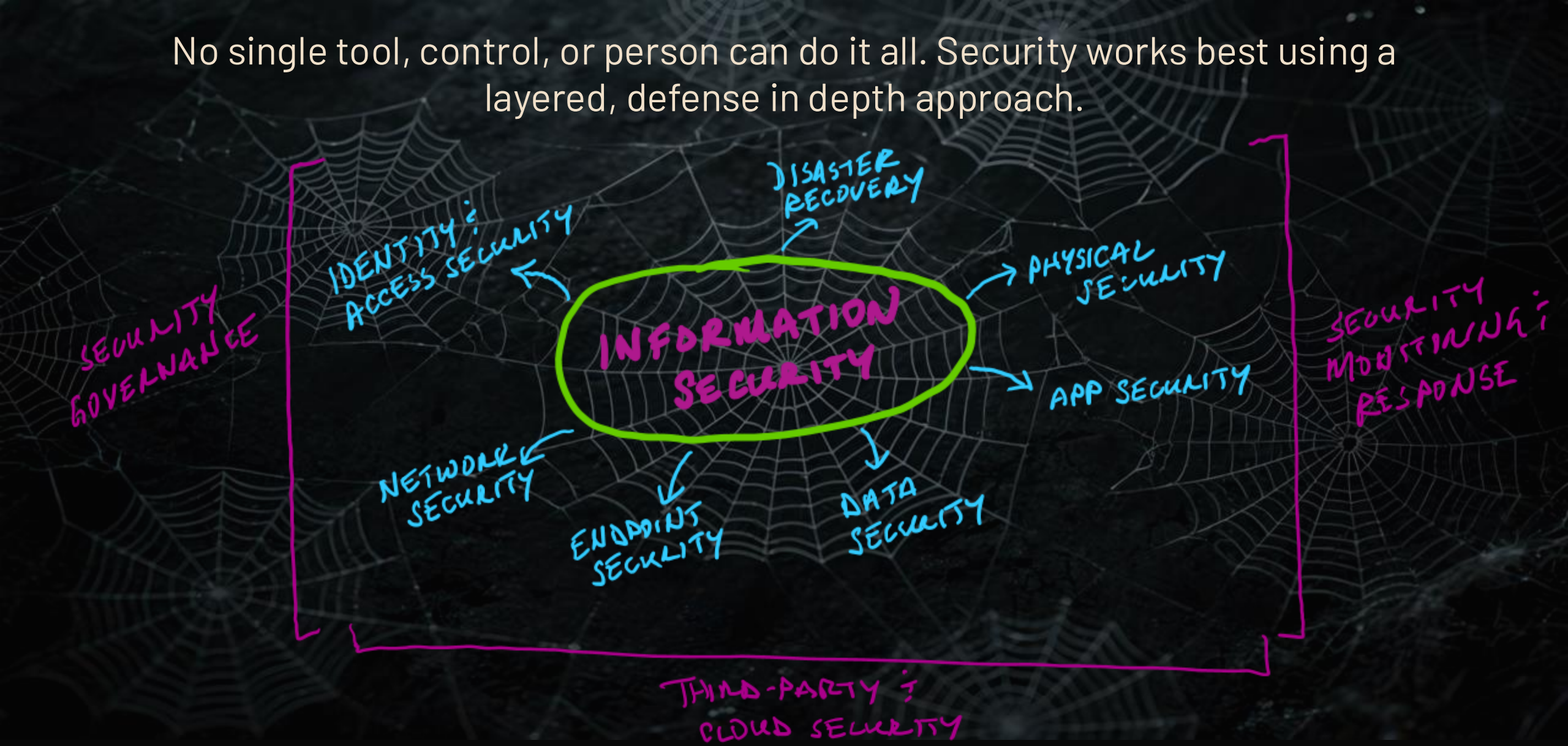
rea BUSINESS ADVISORS

rea BUSINESS ADVISORS

Web of Protection

rea BUSINESS ADVISORS

No single tool, control, or person can do it all. Security works best using a layered, defense in depth approach.

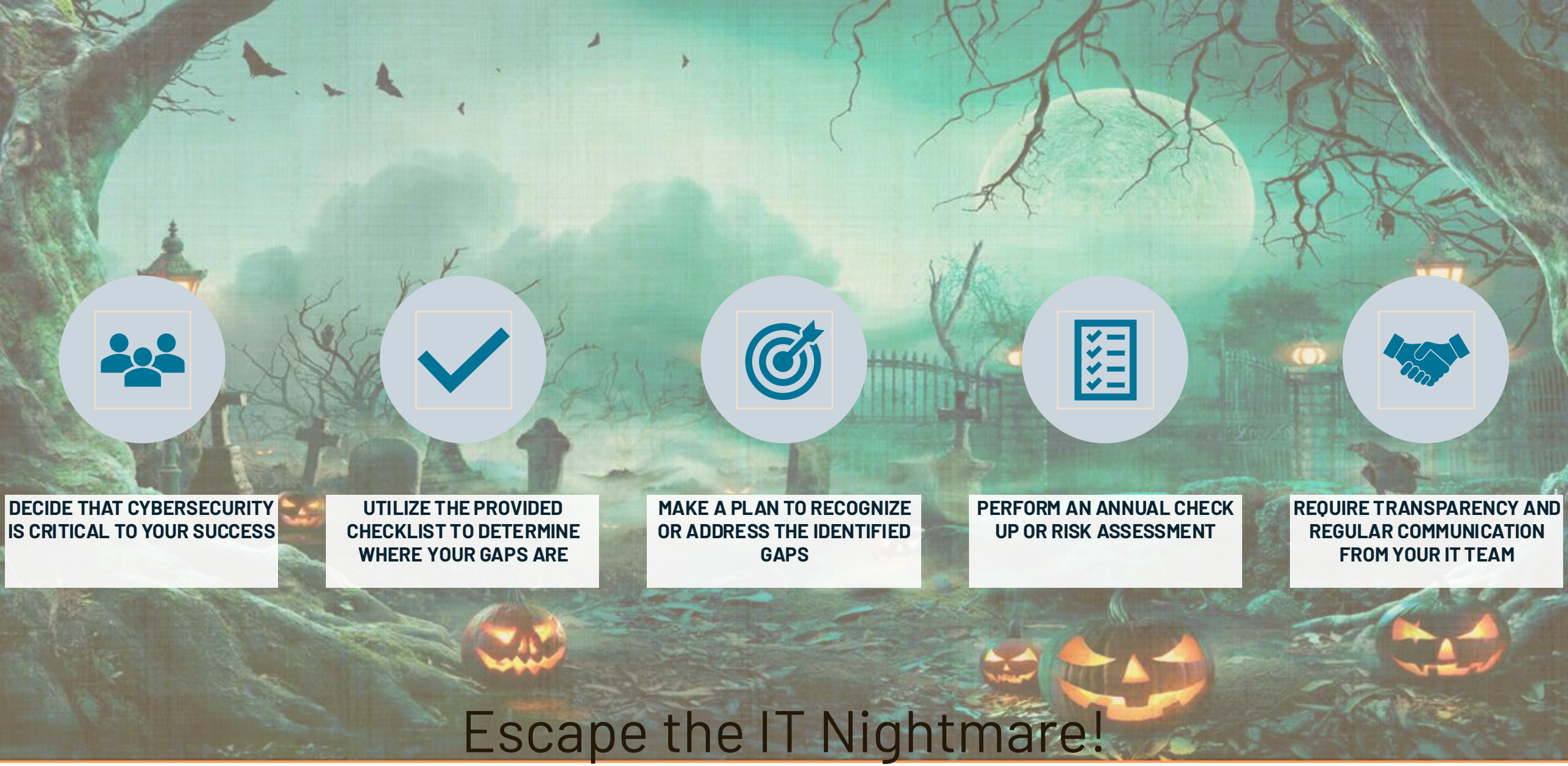


rea BUSINESS ADVISORS

Poll # 3

What actions will you take to ward off the goblins?

rea BUSINESS ADVISORS



Escape the IT Nightmare!

rea BUSINESS ADVISORS

Questions

rea BUSINESS ADVISORS

rea BUSINESS ADVISORS