SouthWest BENEFITS Association | 2021 ANNUAL VIRTUAL CONFERENCE

BENEFIT STRATEGIES FOR THE NEW NORMAL

May 18 – 19 – 20

CYBERSECURITY FOR EMPLOYEE BENEFIT PLANS

CODY GRIFFIN, CPA.CITP, CISA
PARTNER
HOGANTAYLOR TECHNOLOGY

HoganTaylor Technology Security Leaders

Cody Griffin, CPA.CITP, CISA
Partner
HoganTaylor Technology
(501) 221-8121
cgriffin@hogantaylor.com

Adam Prichard, MSCE, CISSP, CEH
Director Cybersecurity Services
HoganTaylor Technology
(501) 221-8121
aprichard@hogantaylor.com

Agenda

- 2020 Security Year in Review
- Identifying the increased Threat Landscape
- DOL-EMBSA Cybersecurity Program Best Practices
- DOL-EMBSA Tips for Hiring A Service Provider
- DOL-EMBSA Online Security Tips
- Review of Assessment tools
- Wrap-up and Questions

2020 Security Year in Review

ANALYZED A RECORD 157,525 INCIDENTS

32,002 MET VERIZON'S QUALITY STANDARDS

3,950 CONFIRMED DATA BREACHES

DBIR Summary of Findings

Figure 2. What tactics are utilized? (Actions)

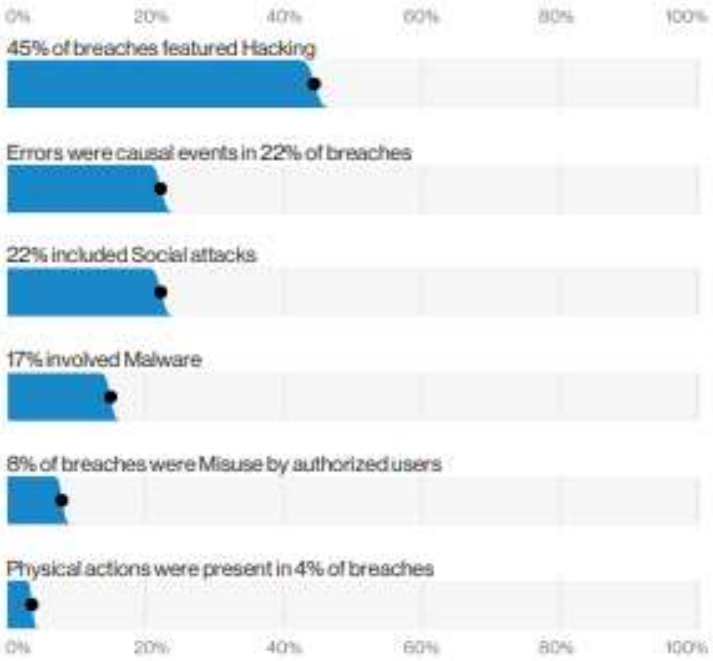


Figure 3. Who's behind the breaches?

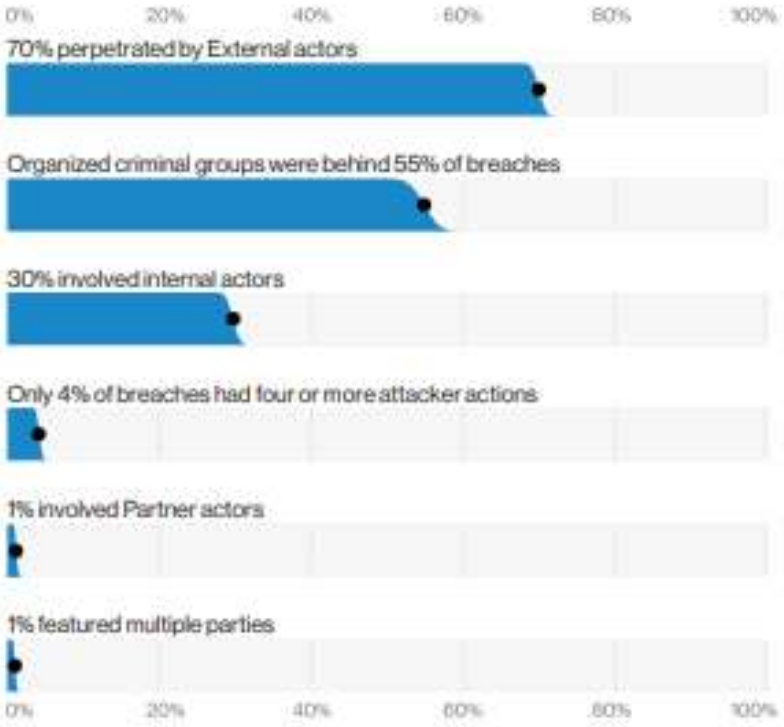
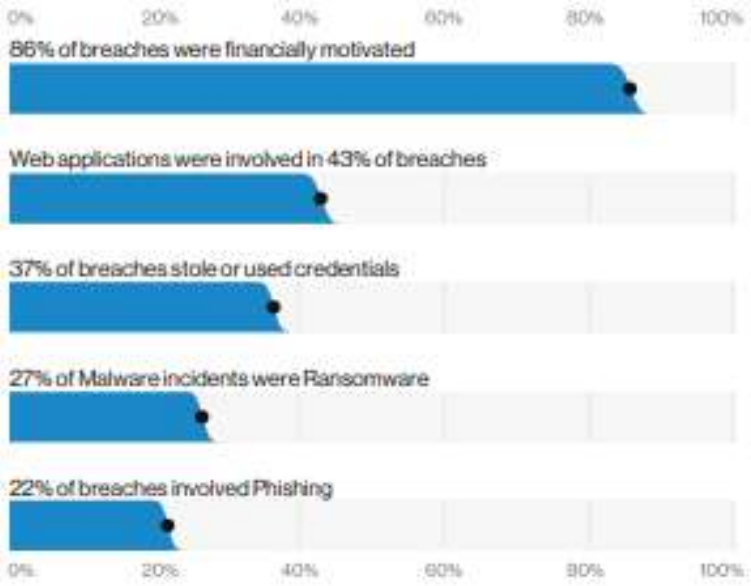


Figure 5. What are the other commonalities?



Financial and Insurance Industry Breakdown

Figure 66. Patterns in Finance and Insurance industry breaches (n = 448)

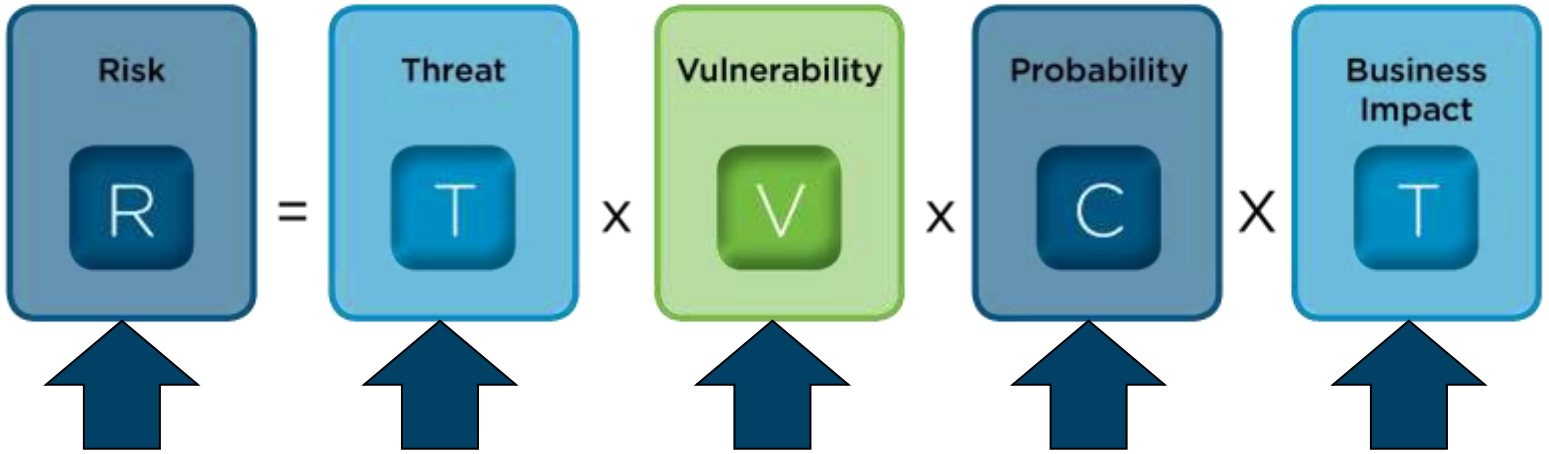
1,509 incidents, 448 with confirmed data disclosure

Threat Actors: External (64%), Internal (35%), Partner (2%), Multiple (1%)

Actor Motives: Financial (91%), Espionage (3%), Grudge (3%)

Figure 67. Top Error varieties in Finance and Insurance industry breaches (n = 109)

Cyber Risk Rising While Working Remote



Risk will be elevated throughout the pandemic

Bad actors using COVID-19 themed attacks to conduct BEC, ransomware, Denial of Service

Attack surface rapidly expanded with work from home / remote connections in support of social distancing

IT staffs are spread thin

IT staffs are supporting users with weaker skills and inadequate tools

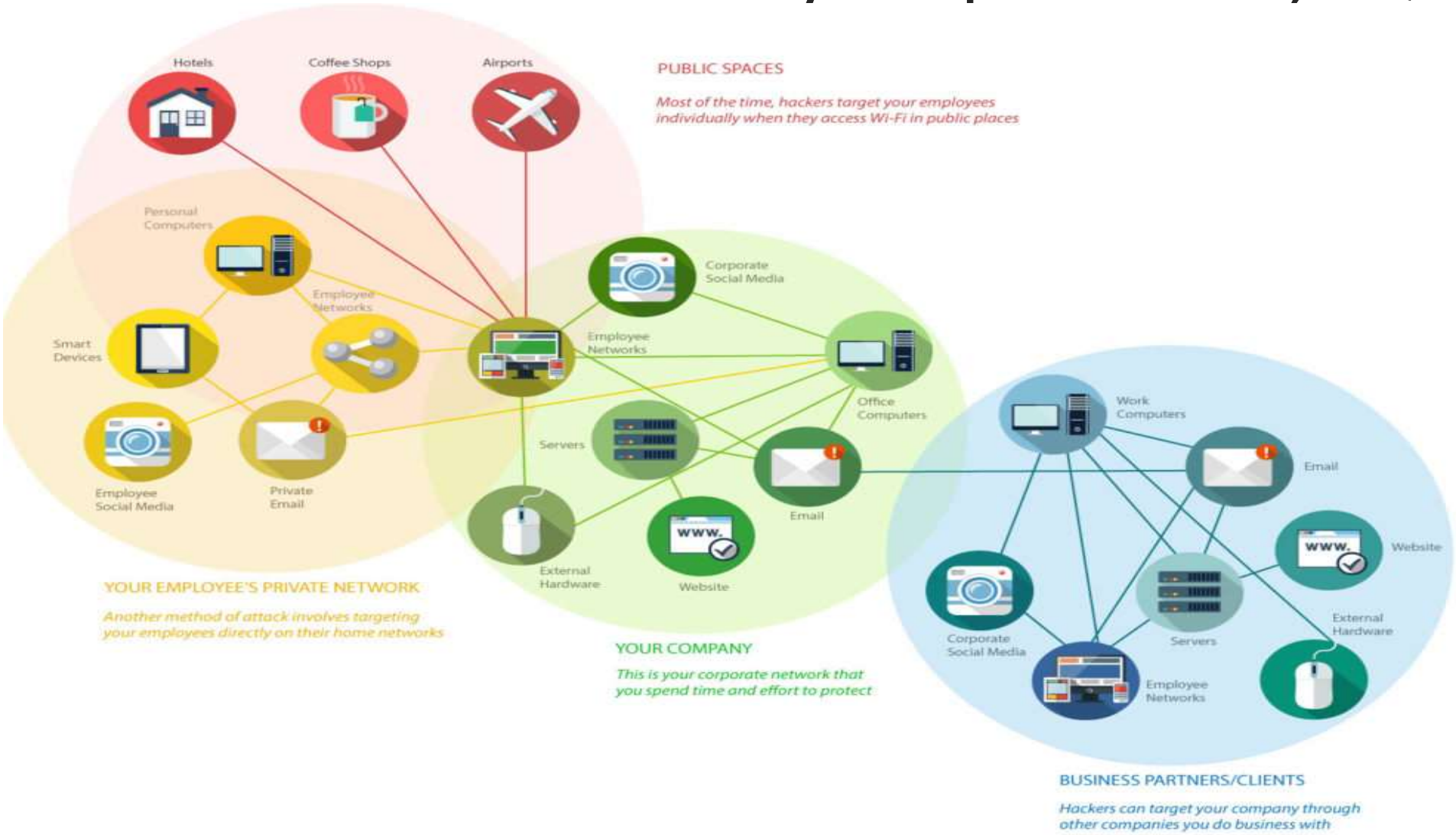
FBI, FTC, Homeland Defense all have published advisories on COVID-19 themed attacks

Electronic storefronts, phone, email systems most businesses only way to serve customers

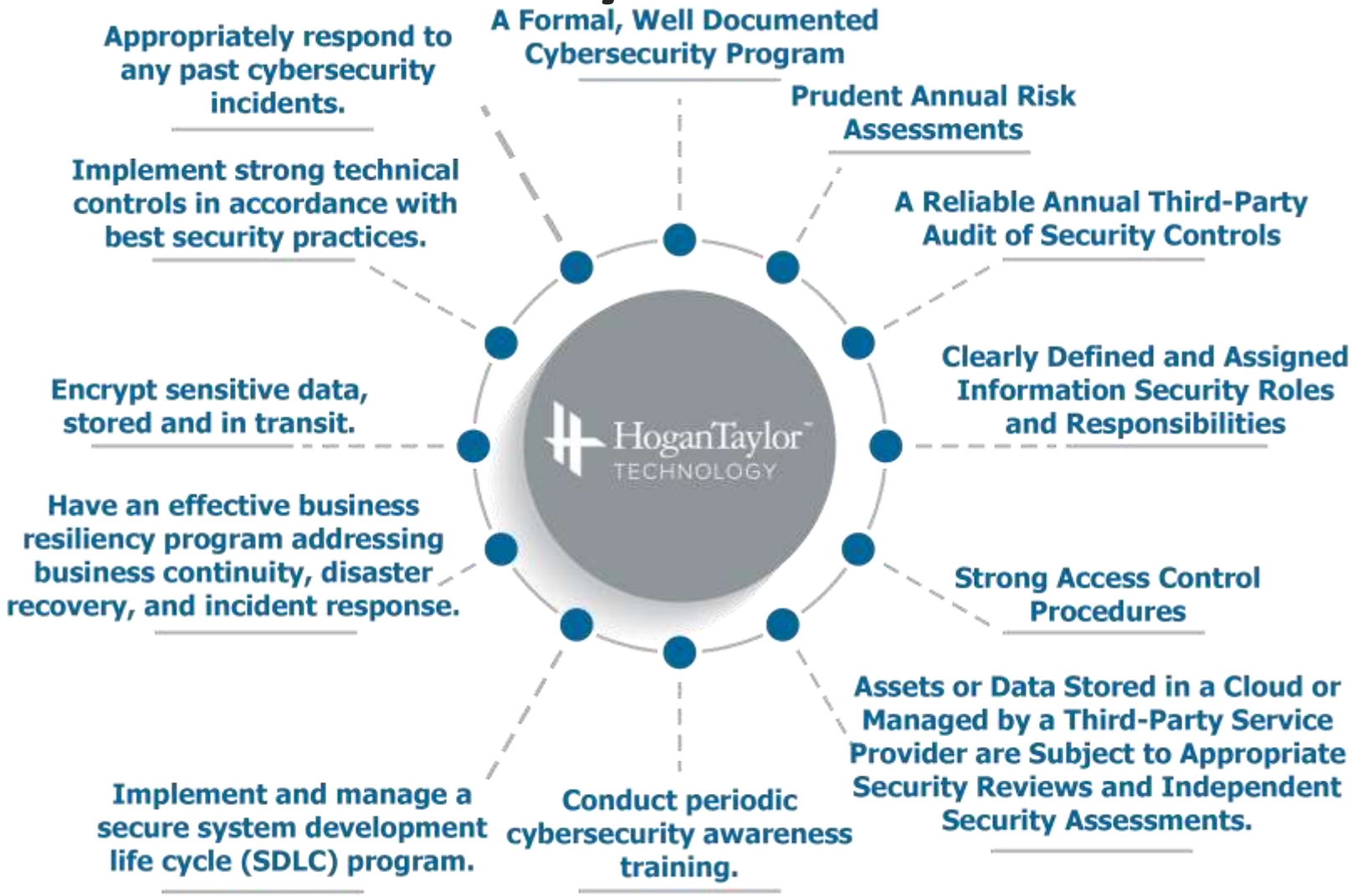
Weak cash flow positions for many firms will magnify a cyber event's impact

Distributed infrastructure may lengthen detecting, response, recover times

Attack Surfaces Greatly Expanded, Quickly



Cybersecurity Best Practices



Tips for Hiring a Service Provider

01 Ask about the service provider's information security standards, practices and policies, and audit results, and compare them to the industry standards adopted by other financial institutions.

02 Ask the service provider how it validates its practices, and what levels of security standards it has met and implemented. Look for contract provisions that give you the right to review audit results demonstrating compliance with the standard.

03 Evaluate the service provider's track record in the industry, including public information regarding information security incidents, other litigation, and legal proceedings related to vendor's services.

04 Ask whether the service provider has experienced past security breaches, what happened, and how the service provider responded.

05 Find out if the service provider has any insurance policies that would cover losses caused by cybersecurity and identity theft breaches (including breaches caused by internal threats, such as misconduct by the service provider's own employees or contractors, and breaches caused by external threats, such as a third party hijacking a plan participants' account).

06 When you contract with a service provider, make sure that the contract requires ongoing compliance with cybersecurity and information security standards – and beware contract provisions that limit the service provider's responsibility for IT security breaches.

Online Security Tips

REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT

USE STRONG AND UNIQUE PASSWORDS

USE MULTI-FACTOR AUTHENTICATION

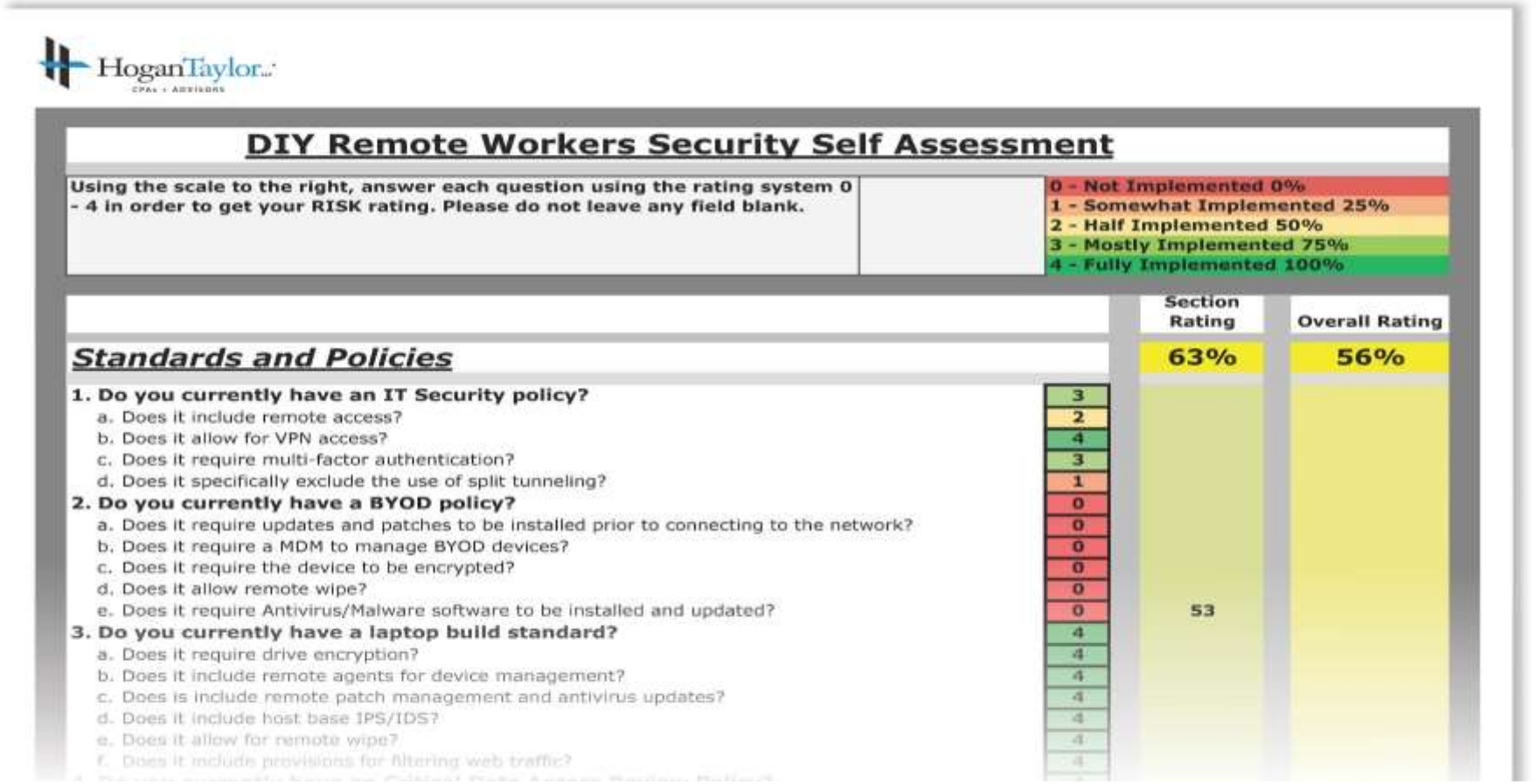
KEEP PERSONAL CONTACT INFORMATION CURRENT

CLOSE OR DELETE UNUSED ACCOUNTS

BE WARY OF FREE WI-FI

BEWARE OF PHISHING ATTACKS

DIY Security Assessment Walk Through



HoganTaylor

DIY Remote Workers Security Self Assessment

Using the scale to the right, answer each question using the rating system 0 - 4 in order to get your RISK rating. Please do not leave any field blank.

0 - Not Implemented 0%
1 - Somewhat Implemented 25%
2 - Half Implemented 50%
3 - Mostly Implemented 75%
4 - Fully Implemented 100%

		Section Rating	Overall Rating
Standards and Policies		63%	56%
1. Do you currently have an IT Security policy?	3		
a. Does it include remote access?	2		
b. Does it allow for VPN access?	4		
c. Does it require multi-factor authentication?	3		
d. Does it specifically exclude the use of split tunneling?	1		
2. Do you currently have a BYOD policy?	0		
a. Does it require updates and patches to be installed prior to connecting to the network?	0		
b. Does it require a MDM to manage BYOD devices?	0		
c. Does it require the device to be encrypted?	0		
d. Does it allow remote wipe?	0		
e. Does it require Antivirus/Malware software to be installed and updated?	0	53	
3. Do you currently have a laptop build standard?	4		
a. Does it require drive encryption?	4		
b. Does it include remote agents for device management?	4		
c. Does is include remote patch management and antivirus updates?	4		
d. Does it include host base IPS/IDS?	4		
e. Does it allow for remote wipe?	4		
f. Does it include provisions for filtering web traffic?	4		

https://info.hogantaylor.com/diy-security-materials

Questions?

Cody Griffin
Partner
HoganTaylor Technology
(501) 221-8121
cgriffin@hogantaylor.com

Adam Prichard
Director Cybersecurity Services
HoganTaylor Technology
(501) 221-8121
aprichard@hogantaylor.com