PERFORMING ASSESSMENTS USING ZERO TRUST PRINCIPLES

YOUR IT COMPLIANCE PARTNER – GO BEYOND THE CHECKLIST

AGENDA

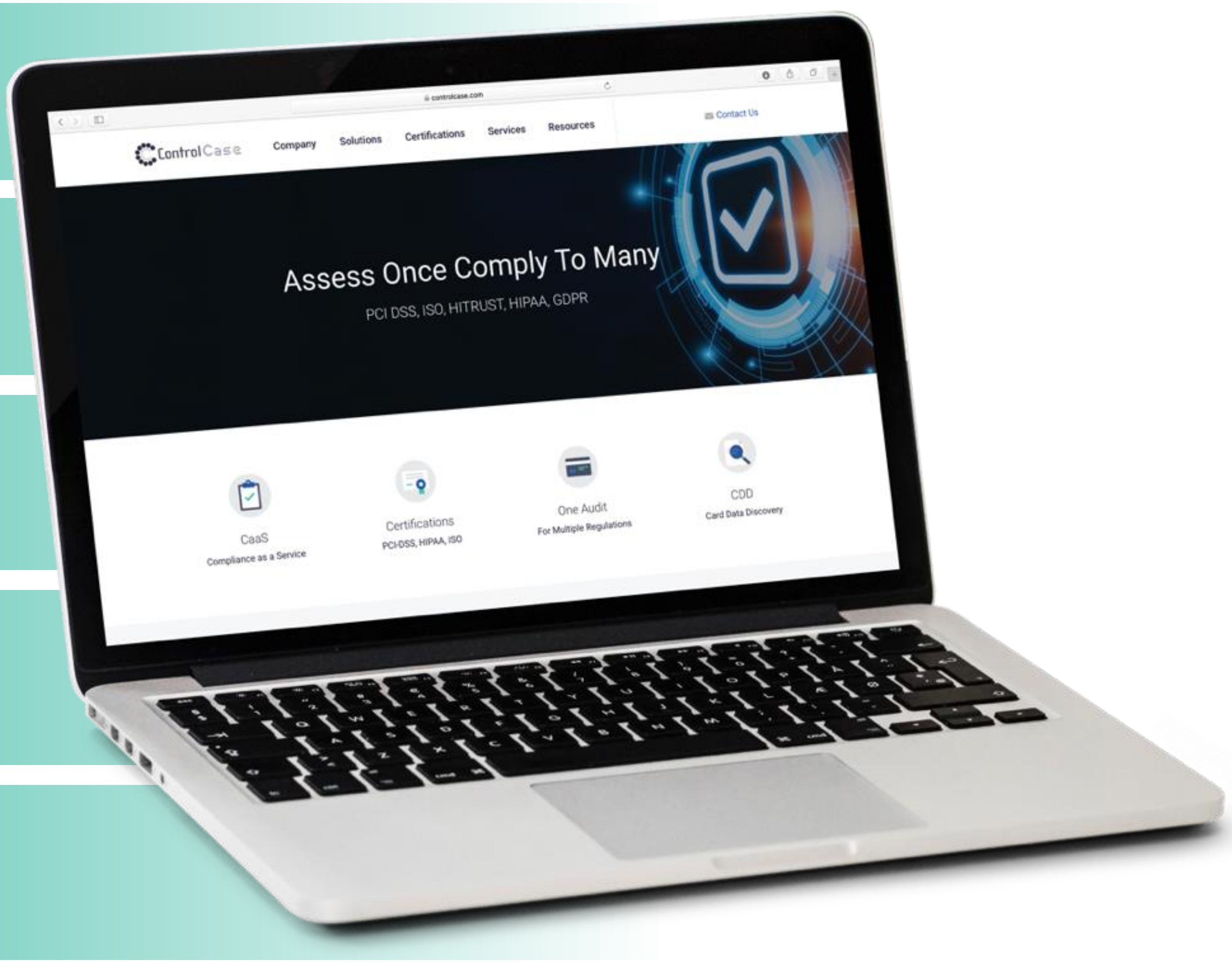
1 Introductions – ControlCase, Tag Cyber, Evolve MGA

2 Current Research

3 What are Zero Trust Principles

4 Implementing Zero Trust Principles in Remote Working Environments

5 Cyber Insurance for Modern Day Exposures



1

INTRODUCTIONS

ControlCase Snapshot

CERTIFICATION AND CONTINUOUS COMPLIANCE SERVICES

Go beyond the auditor’s checklist to:

Dramatically cut the time, cost and burden from becoming certified and maintaining IT compliance.

- Demonstrate compliance more efficiently and cost effectively (cost certainty)
- Improve efficiencies
  - Do more with less resources and gain compliance peace of mind
- Free up your internal resources to focus on their priorities
- Offload much of the compliance burden to a trusted compliance partner

1,000+

CLIENTS

10,000+

IT SECURITY CERTIFICATIONS

275+

SECURITY EXPERTS

TAGCYBER

ANALYSIS

SERVICES

MEDIA

CYBER CORPS

Dr. Edward Amoroso

CEO, TAG Cyber LLC

EVOLVE

- Evolve MGA is the largest “cyber insurance specialist” company in the United States.
- What is cyber insurance? It is hacker insurance for businesses of every size in all industries.
- Evolve MGA underwrites & distributes the broadest cyber insurance policies in the marketplace.
- Offering the largest cyber insurance specialist claims team in the world, made up of best in class forensic experts.
- Service includes “free” exclusive access to top tier cyber risk management services

Michael Costello

Principal, Co-Founder, Evolve

2

CURRENT RESEARCH

Three Key Continuous Security Compliance Requirements

BASED ON RECENT RESEARCH FINDINGS

CONTINUOUS

An effective compliance program for cyber security must provide a stream of continuous, accurate information about posture.

AUTOMATED

Continuous compliance requires an automated platform that collects and processes data in as close to real-time as can be achieved.

INTEGRATED

The best compliance programs are integrated into the systems being measured, versus built as after-the-fact overlays.

3

WHAT ARE ZERO TRUST PRINCIPLES

What are Zero Trust Principles?

Assume You’re at Risk from all Angles:

- Attackers are both internal and external to your network
- No machine, user or organization is automatically trusted
- Strict access controls and least privilege on processes

4

IMPLEMENTING ZERO TRUST PRINCIPLES IN REMOTE WORKING ENVIRONMENTS

Implementing Principles for Remote Working Environments

PEOPLE

- Adopt a partnership approach with all stakeholders
- Implement continuous compliance as an organizational cultural shift.
- Assessors should maintain their structure for an onsite audit but instead use video calling and screen sharing to provide evidence and conduct interviews as a part of the assessment.
- Management/Managers must review user access in terms of privileges, including printing reports at home computers.

Implementing Principles for Remote Working Environments

TECHNOLOGY

- Remote testing (vulnerability assessment / penetration testing/application security testing)
- Sensitive data should only be accessible via secure encrypted channels
- Sensitive data cannot be copied into or transmitted from local systems.
- Automated evidence collection; especially for cloud infrastructures.
- Strong end-user security and access control architecture for remote end-users.

Implementing Principles for Remote Working Environments

PROCESSES

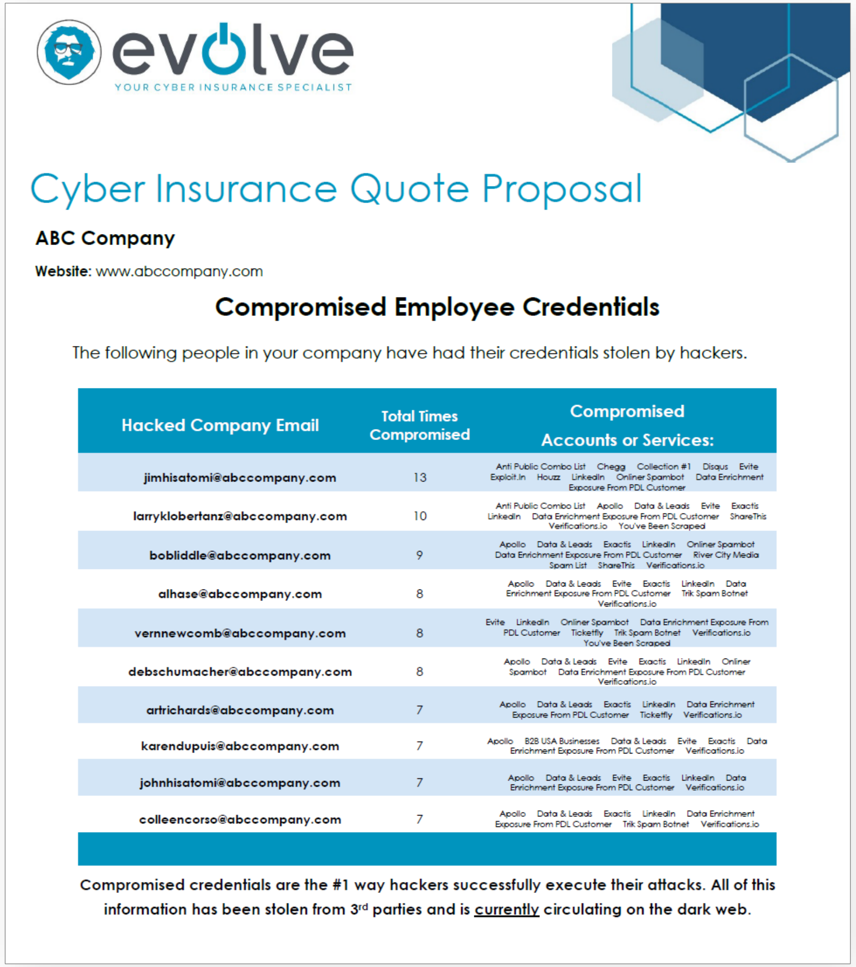
- Additional sampling and checks
- Review and conduct risk assessment process for remote employees
- Automated evidence collection tools and scripts
- Continuous Compliance management

5

CYBER INSURANCE FOR MODERN DAY EXPOSURES

Have you already been hacked?

Dark Web Scanner



evolve
YOUR CYBER INSURANCE SPECIALIST

Cyber Insurance Quote Proposal

ABC Company

Website: www.abccompany.com

Compromised Employee Credentials

The following people in your company have had their credentials stolen by hackers.

Hacked Company Email	Total Times Compromised	Compromised Accounts or Services:
jimhisatomi@abccompany.com	13	Anti Public Combo List Chegg Collection #1 Disqus Evite Exploit.In Houzz LinkedIn Onliner Spambot Data Enrichment Exposure From PDL Customer
larryklobertanz@abccompany.com	10	Anti Public Combo List Apollo Data & Leads Evite Exactis LinkedIn Data Enrichment Exposure From PDL Customer ShareThis Verifications.io You've Been Scraped
bobliddle@abccompany.com	9	Apollo Data & Leads Exactis LinkedIn Onliner Spambot Data Enrichment Exposure From PDL Customer River City Media Spam List ShareThis Verifications.io
alhase@abccompany.com	8	Apollo Data & Leads Evite Exactis LinkedIn Data Enrichment Exposure From PDL Customer Trik Spam Botnet Verifications.io
vernnewcomb@abccompany.com	8	Evite LinkedIn Onliner Spambot Data Enrichment Exposure From PDL Customer Ticketfly Trik Spam Botnet Verifications.io You've Been Scraped
debschumacher@abccompany.com	8	Apollo Data & Leads Evite Exactis LinkedIn Onliner Spambot Data Enrichment Exposure From PDL Customer Verifications.io
artrichards@abccompany.com	7	Apollo Data & Leads Exactis LinkedIn Data Enrichment Exposure From PDL Customer Ticketfly Verifications.io
karendupuis@abccompany.com	7	Apollo B2B USA Businesses Data & Leads Evite Exactis Data Enrichment Exposure From PDL Customer Verifications.io
johnhisatomi@abccompany.com	7	Apollo Data & Leads Evite Exactis LinkedIn Data Enrichment Exposure From PDL Customer Verifications.io
colleencorso@abccompany.com	7	Apollo Data & Leads Exactis LinkedIn Data Enrichment Exposure From PDL Customer Trik Spam Botnet Verifications.io

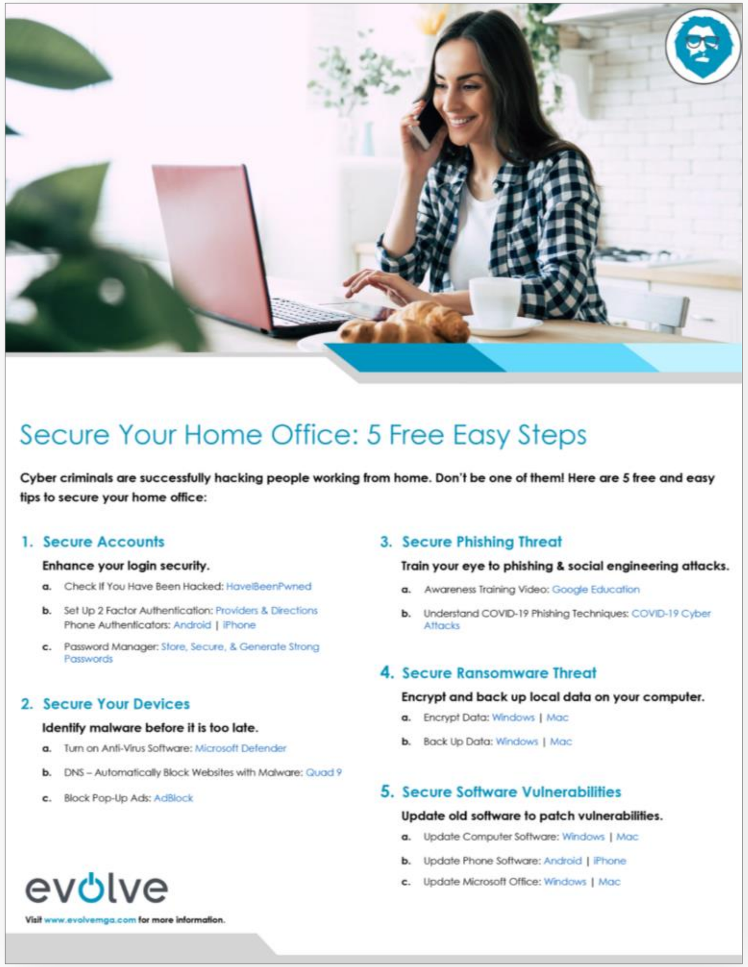
Compromised credentials are the #1 way hackers successfully execute their attacks. All of this information has been stolen from 3rd parties and is currently circulating on the dark web.

Successful Cyberattacks = Human Based Error

Ransomware

Fund Transfer Fraud

Secure Your Home Office



Secure Your Home Office: 5 Free Easy Steps

Cyber criminals are successfully hacking people working from home. Don't be one of them! Here are 5 free and easy tips to secure your home office:

1. Secure Accounts

Enhance your login security.

a. Check If You Have Been Hacked: HaveIBeenPwned

b. Set Up 2 Factor Authentication: Providers & Directions
Phone Authenticators: Android | iPhone

c. Password Manager: Store, Secure, & Generate Strong Passwords

2. Secure Your Devices

Identify malware before it is too late.

a. Turn on Anti-Virus Software: Microsoft Defender

b. DNS – Automatically Block Websites with Malware: Quad 9

c. Block Pop-Up Ads: AdBlock

3. Secure Phishing Threat

Train your eye to phishing & social engineering attacks.

a. Awareness Training Video: Google Education

b. Understand COVID-19 Phishing Techniques: COVID-19 Cyber Attacks

4. Secure Ransomware Threat

Encrypt and back up local data on your computer.

a. Encrypt Data: Windows | Mac

b. Back Up Data: Windows | Mac

5. Secure Software Vulnerabilities

Update old software to patch vulnerabilities.

a. Update Computer Software: Windows | Mac

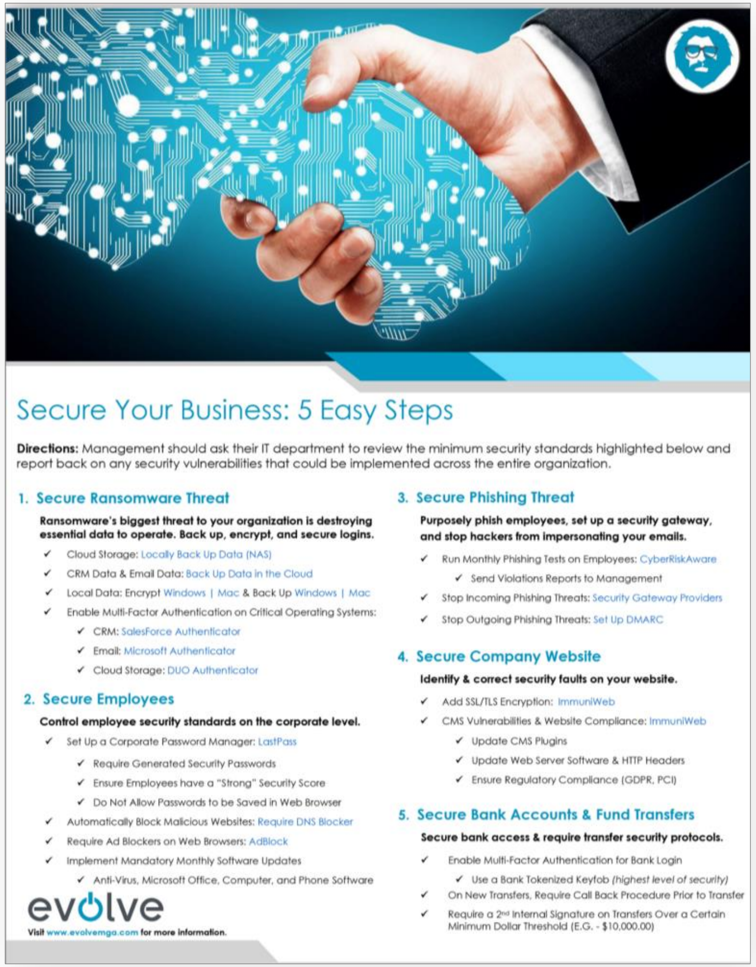
b. Update Phone Software: Android | iPhone

c. Update Microsoft Office: Windows | Mac

evolve

Visit www.evolvemga.com for more information.

Secure Your Business



Secure Your Business: 5 Easy Steps

Directions: Management should ask their IT department to review the minimum security standards highlighted below and report back on any security vulnerabilities that could be implemented across the entire organization.

1. Secure Ransomware Threat

Ransomware's biggest threat to your organization is destroying essential data to operate. Back up, encrypt, and secure logins.

- ✓ Cloud Storage: Locally Back Up Data (NAS)
- ✓ CRM Data & Email Data: Back Up Data in the Cloud
- ✓ Local Data: Encrypt Windows | Mac & Back Up Windows | Mac
- ✓ Enable Multi-Factor Authentication on Critical Operating Systems:
  - ✓ CRM: SalesForce Authenticator
  - ✓ Email: Microsoft Authenticator
  - ✓ Cloud Storage: DUO Authenticator

2. Secure Employees

Control employee security standards on the corporate level.

- ✓ Set Up a Corporate Password Manager: LastPass
  - ✓ Require Generated Security Passwords
  - ✓ Ensure Employees have a "Strong" Security Score
  - ✓ Do Not Allow Passwords to be Saved in Web Browser
- ✓ Automatically Block Malicious Websites: Require DNS Blocker
- ✓ Require Ad Blockers on Web Browsers: AdBlock
- ✓ Implement Mandatory Monthly Software Updates
  - ✓ Anti-Virus, Microsoft Office, Computer, and Phone Software

evolve

Visit www.evolvemga.com for more information.

3. Secure Phishing Threat

Purposely phish employees, set up a security gateway, and stop hackers from impersonating your emails.

- ✓ Run Monthly Phishing Tests on Employees: CyberRiskAware
  - ✓ Send Violations Reports to Management
- ✓ Stop Incoming Phishing Threats: Security Gateway Providers
- ✓ Stop Outgoing Phishing Threats: Set Up DMARC

4. Secure Company Website

Identify & correct security faults on your website.

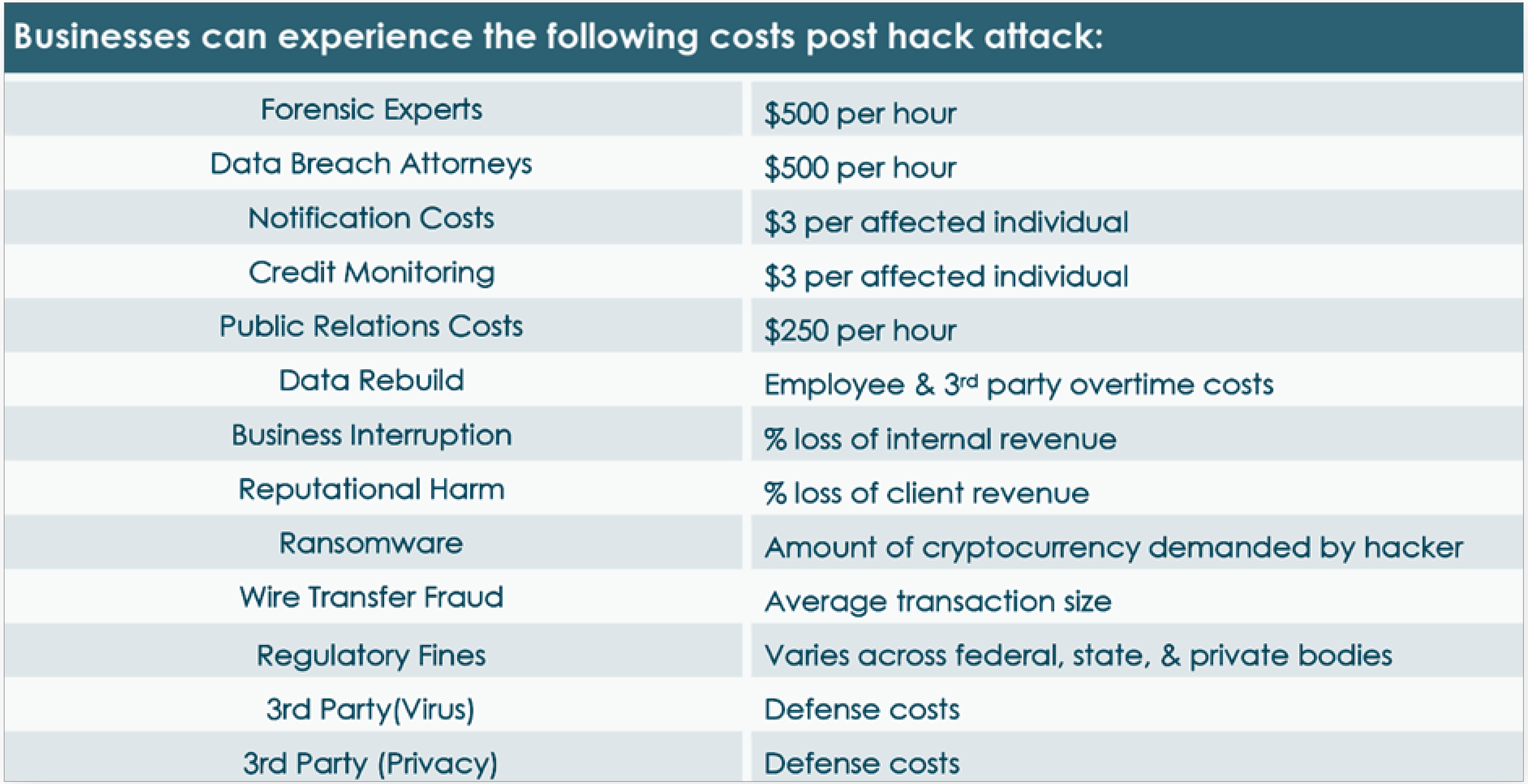
- ✓ Add SSL/TLS Encryption: ImmuniWeb
- ✓ CMS Vulnerabilities & Website Compliance: ImmuniWeb
  - ✓ Update CMS Plugins
  - ✓ Update Web Server Software & HTTP Headers
  - ✓ Ensure Regulatory Compliance (GDPR, PCI)

5. Secure Bank Accounts & Fund Transfers

Secure bank access & require transfer security protocols.

- ✓ Enable Multi-Factor Authentication for Bank Login
  - ✓ Use a Bank Tokenized Keyfob *(highest level of security)*
- ✓ On New Transfers, Require Call Back Procedure Prior to Transfer
- ✓ Require a 2nd Internal Signature on Transfers Over a Certain Minimum Dollar Threshold (E.G. - $10,000.00)

The Value of Cyber Insurance



Businesses can experience the following costs post hack attack:	
Forensic Experts	$500 per hour
Data Breach Attorneys	$500 per hour
Notification Costs	$3 per affected individual
Credit Monitoring	$3 per affected individual
Public Relations Costs	$250 per hour
Data Rebuild	Employee & 3rd party overtime costs
Business Interruption	% loss of internal revenue
Reputational Harm	% loss of client revenue
Ransomware	Amount of cryptocurrency demanded by hacker
Wire Transfer Fraud	Average transaction size
Regulatory Fines	Varies across federal, state, & private bodies
3rd Party(Virus)	Defense costs
3rd Party (Privacy)	Defense costs

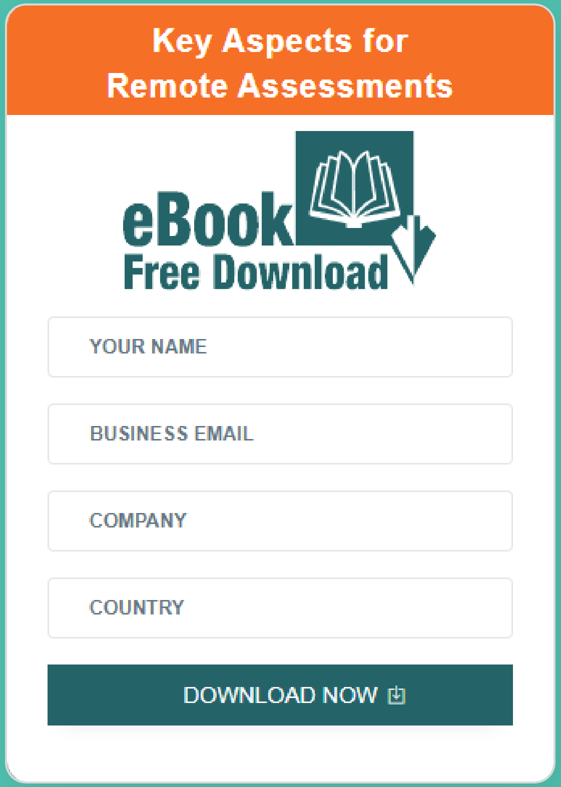
5

Q&A

Access Now - Free Ebook

PERFORMING PCI DSS ASSESSMENTS USING ZERO TRUST PRINCIPLES

https://www.controlcase.com/free-pci-ebook/



Key Aspects for Remote Assessments