bis
BUSINESS INFORMATION SOLUTIONS

Getting IT done.

Hackers Exposed! What You Can Do as a Business Owner to Protect Against Cyber Threats

bis
BUSINESS INFORMATION SOLUTIONS
We Get IT Done!

EVENT AGENDA

Cybersecurity Lunch-n-Learn

11:30 – 11:40 AM

Registration & Introduction

11:40 AM – 12:50 PM

Hackers Exposed! What You Can Do as a Business Owner to Protect Against Cyber Threats

Speaker: Phillip Long, CEO of BIS and Cyber Fortress (see his bio on page 3)

12:50 – 12:55 PM

Q & A

Please fill out the survey at this time.

12:55 – 1:00 PM

Giveaway!

Dear Guest,

I would like to personally thank you for taking the time to attend our cybersecurity event today. As a fellow businessman and entrepreneur, I understand the value of time and I appreciate your investment.

Cybersecurity is one of the largest challenges businesses are facing today due to an increase in cyber attacks and remote workers. Over the last 20 years, I have worked to develop this multi-layered approach that we are going to discuss today.

It is our company's goal to enable our clients to have a better technology partner than their competitors. We fully recognize that your success not only ensures our success, but also validates it. If there is any way that I can help you and your business, please don't hesitate to contact me.

All the best!

Respectfully,

Phillip D. Long
CEO
BIS Technology Group
www.askbis.com
plong@askbis.com

Who is Phillip Long?

Phillip Long is a technology guru and entrepreneur with both Certified Information Systems Security Professional (CISSP) and Cybersecurity Maturity Model Certifications (CMMC) who specializes in providing technology solutions and security consulting to businesses along the Gulf Coast. Phillip has more than 20 years of experience in the technology field. After forming Business Information Solutions in 2001, the company has grown immensely under his guidance.

As a CEO and entrepreneur, Phillip has expanded his drive for knowledge and growth into a desire to share his experience and passion with others in the business world. This has led him to participate in multiple peer groups with numerous industry leaders in order to learn from their success and the challenges they have overcome.

“I am constantly expanding my knowledge in business and technology. Whether it’s through reading books authored by industry leaders, participating in peer groups or attending conferences around the country. I’m never satisfied with what I know, because I always want to know and understand more. And I want to, in turn, share my knowledge, experience and understanding with others,” Long said.

Long has a firm belief that as a leader, your success isn’t measured just by what you achieve, but by what those around you achieve. And thus, he finds his motivation in seeing those around him learn, grow and reach their maximum potential. He also values the knowledge he gains from individuals, businesses and clients as they overcome their own challenges.

“At the end of the day, we’re not just in the business of digital marketing and IT support, we’re in the business of success. My focus has always been and will always be to help clients achieve success in any way and every way possible.

NOTES

Hackers Exposed! What a Business Owner Can Do to Protect Against Cyber Threats

NOTES

Hackers Exposed! What a Business Owner Can Do to Protect Against Cyber Threats

HACKERS EXPOSED!

What a Business Owner Can Do to Protect Against Cyber Threats

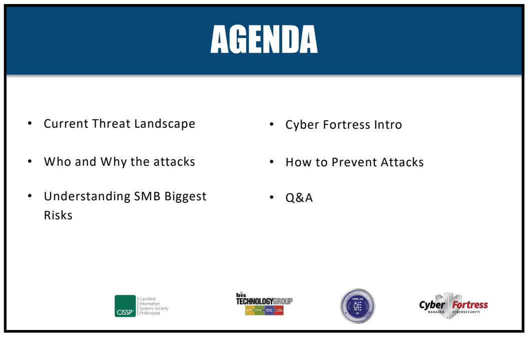
1

WHO IS PHILLIP LONG?

"I am a technologist and entrepreneur who specializes in providing **technology solutions** and **security consulting** to businesses along the Gulf Coast."

- Worked In The IT Industry For Over 20 Years
- 600+ Clients From Gulfport to Gulf Breeze
- Current Owner of 5 Businesses
- Certified Information Systems Security Professional
- CMMC Register Practitioner

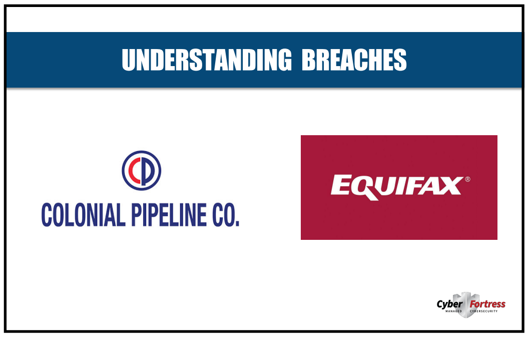
2



AGENDA

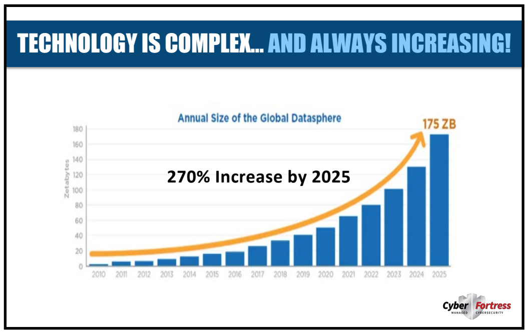
- Current Threat Landscape
- Who and Why the attacks
- Understanding SMB Biggest Risks
- Cyber Fortress Intro
- How to Prevent Attacks
- Q&A

3



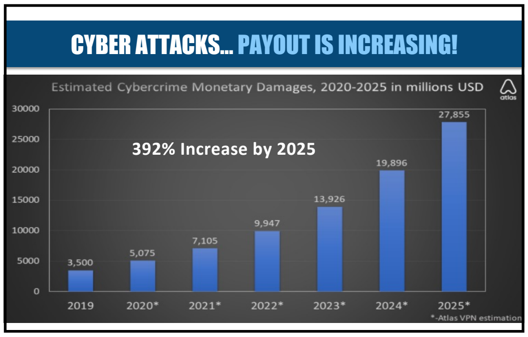
UNDERSTANDING BREACHES

4



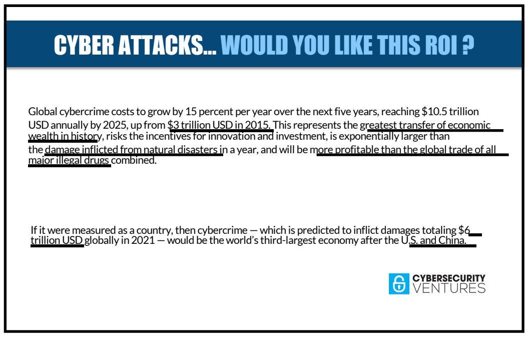
TECHNOLOGY IS COMPLEX… AND ALWAYS INCREASING!

5



CYBER ATTACKS… PAYOUT IS INCREASING!

6



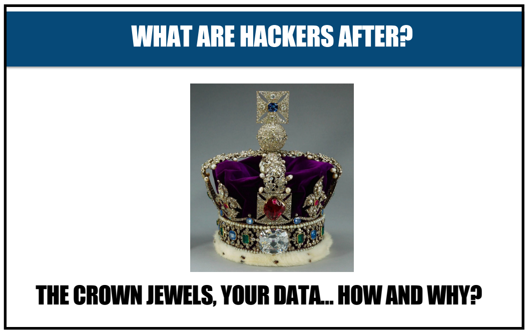
CYBER ATTACKS… WOULD YOU LIKE THIS ROI ?

Global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China.

CYBERSECURITY VENTURES

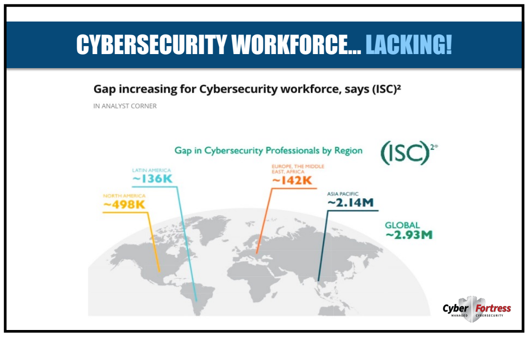
7



WHAT ARE HACKERS AFTER?

THE CROWN JEWELS, YOUR DATA… HOW AND WHY?

8

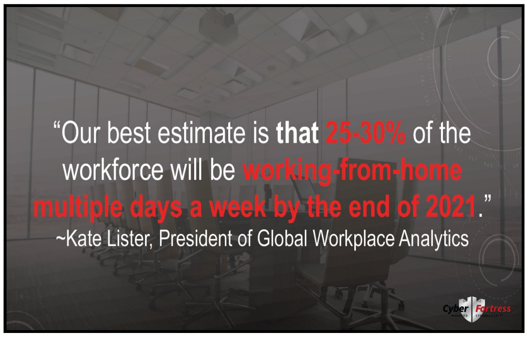


CYBERSECURITY WORKFORCE… LACKING!

Gap increasing for Cybersecurity workforce, says (ISC)²

IN ANALYST CORNER

9

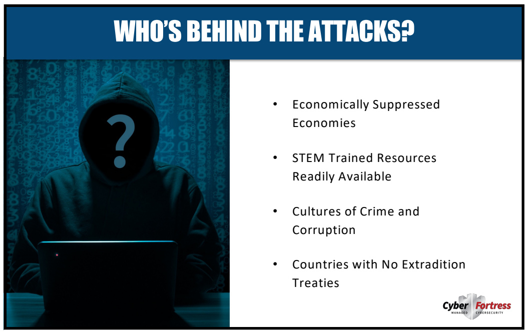


“Our best estimate is that 25-30% of the workforce will be working-from-home multiple days a week by the end of 2021.”

~Kate Lister, President of Global Workplace Analytics

Cyber Fortress

10

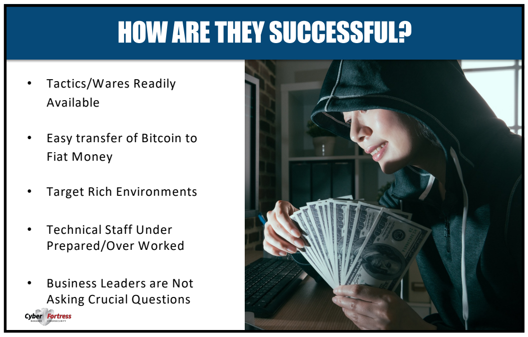


WHO'S BEHIND THE ATTACKS?

- Economically Suppressed Economies
- STEM Trained Resources Readily Available
- Cultures of Crime and Corruption
- Countries with No Extradition Treaties

Cyber Fortress

11



HOW ARE THEY SUCCESSFUL?

- Tactics/Wares Readily Available
- Easy transfer of Bitcoin to Fiat Money
- Target Rich Environments
- Technical Staff Under Prepared/Over Worked
- Business Leaders are Not Asking Crucial Questions

Cyber Fortress

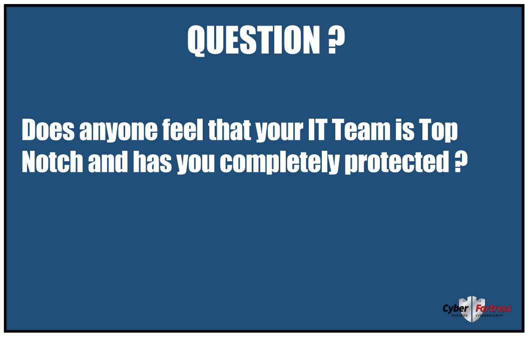
12

WHAT ARE YOUR EMPLOYEES DOING TO PUT YOUR COMPANY AT RISK?

13

THE MULTI-LAYERED SECURITY APPROACH

14



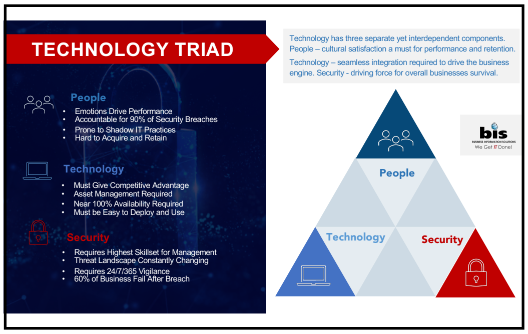
QUESTION ?

Does anyone feel that your IT Team is Top Notch and has you completely protected ?

15

ARE YOU LEAVING YOUR CAR DOORS UNLOCKED?

16



TECHNOLOGY TRIAD

People

- Emotions Drive Performance
- Accountable for 90% of Security Breaches
- Prone to Shadow IT Practices
- Hard to Acquire and Retain

Technology

- Must Give Competitive Advantage
- Asset Management Required
- Near 100% Availability Required
- Must be Easy to Deploy and Use

Security

- Requires Highest Skillset for Management
- Threat Landscape Constantly Changing
- Requires 24/7/365 Vigilance
- 60% of Business Fail After Breach

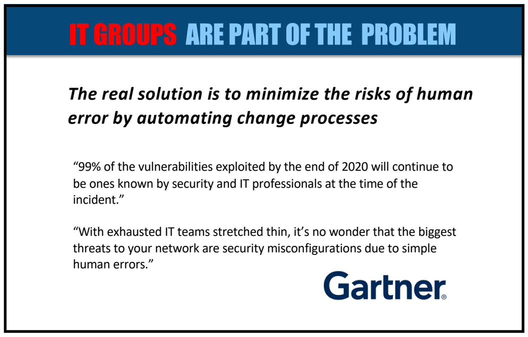
Technology has three separate yet interdependent components. People – cultural satisfaction a must for performance and retention.

Technology – seamless integration required to drive the business engine. Security - driving force for overall businesses survival.

17

WHAT YOU CAN DO AS A BUSINESS OWNER...

18



IT GROUPS ARE PART OF THE PROBLEM

The real solution is to minimize the risks of human error by automating change processes

"99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident."

"With exhausted IT teams stretched thin, it's no wonder that the biggest threats to your network are security misconfigurations due to simple human errors."

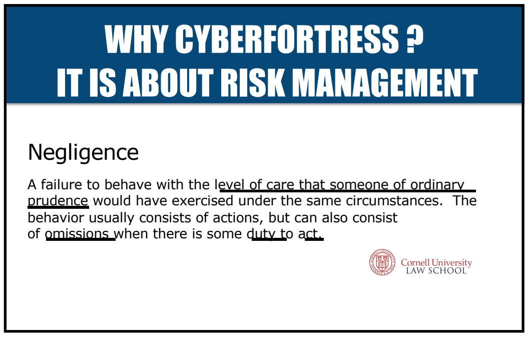
Gartner

19

WHAT IS CYBERFORTRESS ?

Cyber Fortress
MANAGED CYBERSECURITY

20



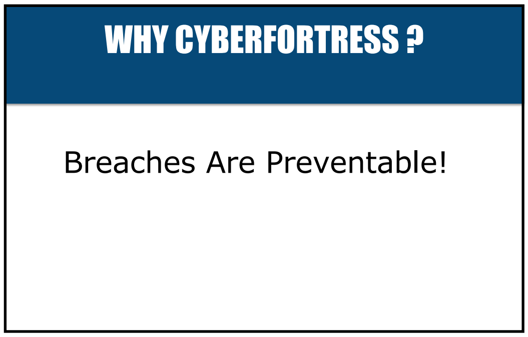
WHY CYBERFORTRESS ? IT IS ABOUT RISK MANAGEMENT

Negligence

A failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances. The behavior usually consists of actions, but can also consist of omissions when there is some duty to act.

Cornell University LAW SCHOOL

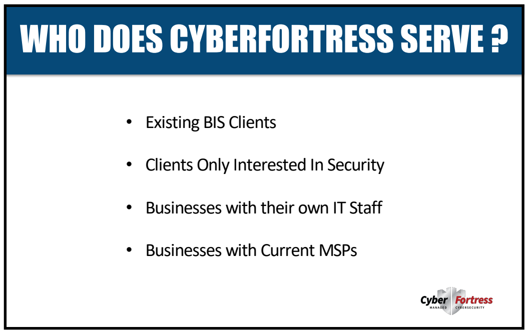
21



WHY CYBERFORTRESS ?

Breaches Are Preventable!

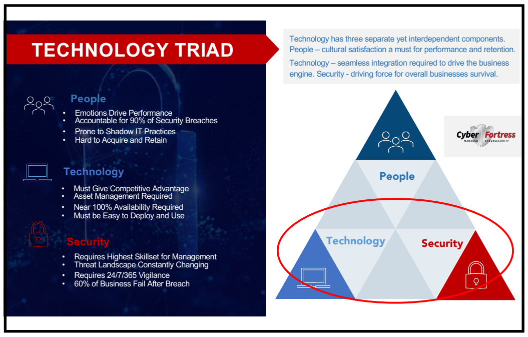
22



WHO DOES CYBERFORTRESS SERVE ?

- Existing BIS Clients
- Clients Only Interested In Security
- Businesses with their own IT Staff
- Businesses with Current MSPs

23



TECHNOLOGY TRIAD

People

- Emotions Drive Performance
- Accountable for 90% of Security Breaches
- Prone to Shadow IT Practices
- Hard to Acquire and Retain

Technology

- Must Give Competitive Advantage
- Asset Management Required
- Near 100% Availability Required
- Must be Easy to Deploy and Use

Security

- Requires Highest Skillset for Management
- Threat Landscape Constantly Changing
- Requires 24/7/365 Vigilance
- 60% of Business Fail After Breach

Technology has three separate yet interdependent components. People – cultural satisfaction a must for performance and retention.

Technology – seamless integration required to drive the business engine. Security - driving force for overall businesses survival.

24

ZERO TRUST

Client

- Too much trust in IT Department/Guy
- Too busy to keep up with technologies
- Low technology acumen

Managed Service Provider (MSP)

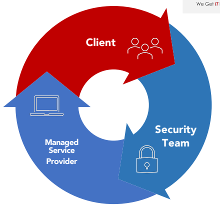
- IT department is overloaded
- IT is focused on up-time
- No ongoing training cybersecurity training

Security Team (Cyber Fortress)

- Scheduled Technical Business Reviews
- 24/7/365 Endpoint Detection & Response with Reporting
- Technology Roadmapping

A zero Trust Relationship has become a necessity with today's threat landscape. Zero Trust requires that all parties work together for the common good of the business but have defined responsibilities and deliverables.

bis
BUSINESS INFORMATION SOLUTIONS
We Get IT Done!



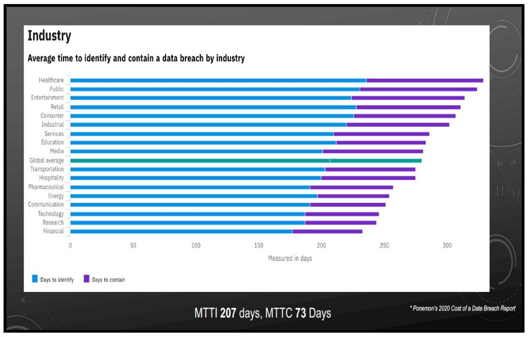
25

POP QUIZ!

How long on average does it take for an organization to identify they've been breached?

A. 7 hours
B. 7 days
C. 7 weeks
D. 7 months

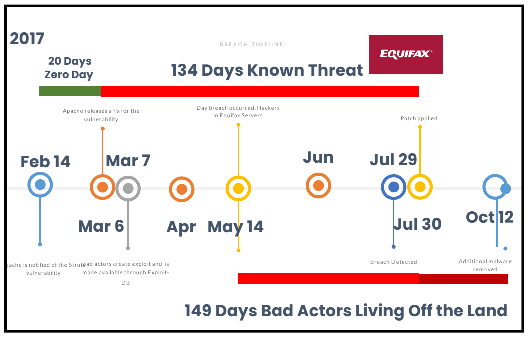
26



MTTI **207** days, MTTC **73** Days

* Ponemon's 2020 Cost of a Data Breach Report

27



2017

BREACH TIMELINE

20 Days Zero Day

134 Days Known Threat

Feb 14 – ache is notified of the Struts vulnerability

Mar 6 – Bad actors create exploit and is made available through Exploit-DB

Mar 7 – Apache releases a fix for the vulnerability

Apr

May 14 – Day breach occurred. Hackers in Equifax Servers

Jun

Jul 29 – Breach Detected

Jul 30 – Patch applied

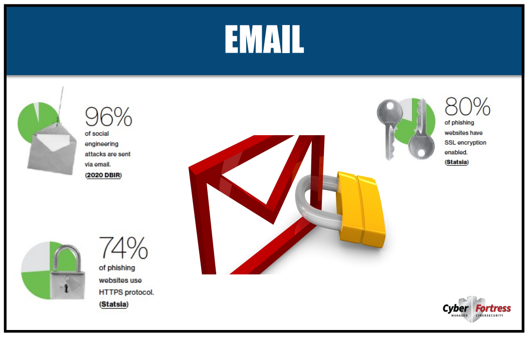
Oct 12 – Additional malware removed

149 Days Bad Actors Living Off the Land

28

WHAT IS YOUR BIGGEST RISKS ?

29



EMAIL

96% of social engineering attacks are sent via email. (2020 DBIR)

74% of phishing websites use HTTPS protocol. (Statsia)

80% of phishing websites have SSL encryption enabled. (Statsia)

30

MISCONFIGURED FIREWALL ?

"Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws."

Gartner

31

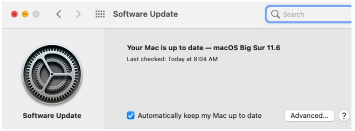
CONTROLLING AUTHENTICATION

32

SYSTEMS PATCHING ?

"57% of cyberattack victims stated that applying a patch would have prevented the attack. 34% say they knew about the vulnerability before the attack."

Ponemon Institute



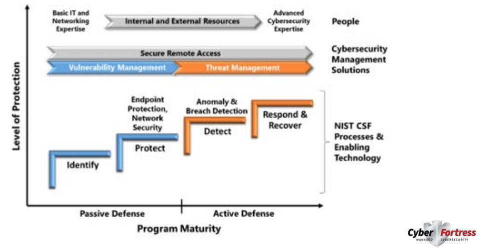
Your Mac is up to date — macOS Big Sur 11.6

Last checked: Today at 8:04 AM

☑ Automatically keep my Mac up to date

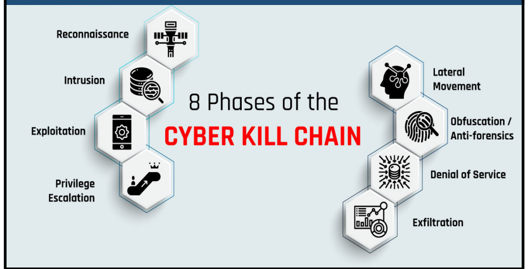
33

END POINT DETECTION AND RESPONSE


Basic IT and Networking Expertise
Internal and External Resources
Advanced Cybersecurity Expertise
People
Secure Remote Access
Vulnerability Management
Threat Management
Cybersecurity Management Solutions
Endpoint Protection, Network Security
Anomaly & Breach Detection
Respond & Recover
Detect
Protect
Identify
NIST CSF Processes & Enabling Technology
Level of Protection
Passive Defense
Active Defense
Program Maturity
Cyber Fortress MANAGED CYBERSECURITY

34

HOW IT IS DONE - CYBER KILL CHAIN



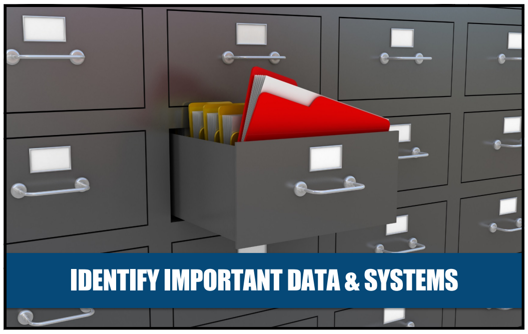
35

RANSOM & EXTORTION

36

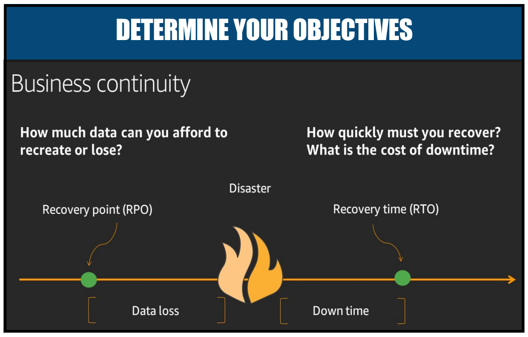
HERE'S WHAT YOU DO IF YOU DON'T WANT TO PAY…

37



IDENTIFY IMPORTANT DATA & SYSTEMS

38



DETERMINE YOUR OBJECTIVES

Business continuity

How much data can you afford to recreate or lose?

How quickly must you recover? What is the cost of downtime?

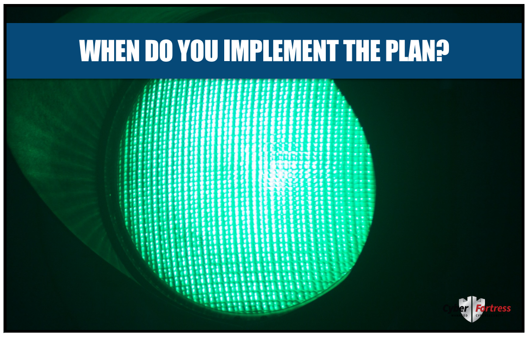
39

WRITE A DISASTER RECOVERY PLAN

40

INCIDENT RESPONSE PLAN

41



WHEN DO YOU IMPLEMENT THE PLAN?

42

COMPONENTS OF A GOOD PLAN

- □ BACKUP EVERYTHING
- □ FAST ENDPOINT DETECTION & RESPONSE
- □ GREAT CHANGE MANAGEMENT SYSTEM
- □ PERIODIC WELL BABY CHECKUP
- □ CONSISTENT TECHNOLOGY ROADMAPPING
- □ ONGOING FIRE DRILLS

43

DON'T FORGET TO BACK UP MICROSOFT 365!

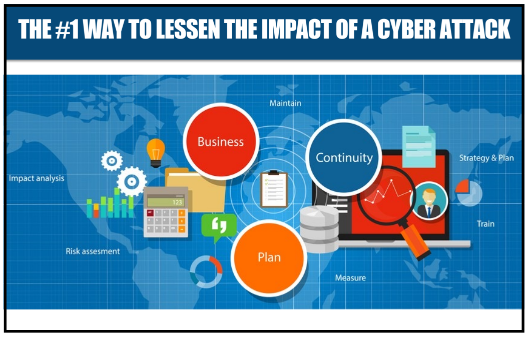
No guarantee against data loss

> Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. **We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.**

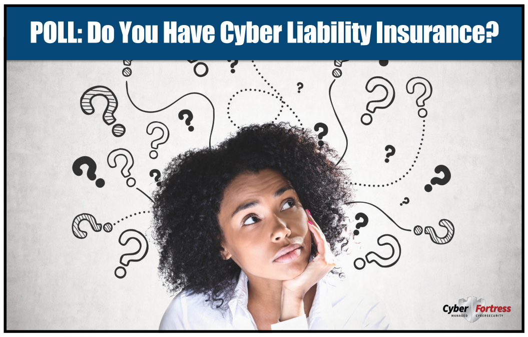
- Microsoft Services Agreement, Section 6b

44

THE #1 WAY TO LESSEN THE IMPACT OF A CYBER ATTACK

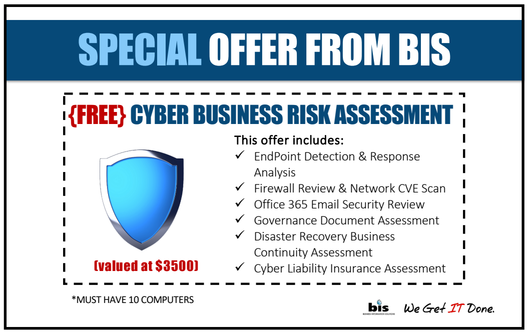


45



POLL: Do You Have Cyber Liability Insurance?

46



SPECIAL OFFER FROM BIS

{FREE} CYBER BUSINESS RISK ASSESSMENT

This offer includes:

- ✓ EndPoint Detection & Response Analysis
- ✓ Firewall Review & Network CVE Scan
- ✓ Office 365 Email Security Review
- ✓ Governance Document Assessment
- ✓ Disaster Recovery Business Continuity Assessment
- ✓ Cyber Liability Insurance Assessment

(valued at $3500)

*MUST HAVE 10 COMPUTERS

bis We Get IT Done.

47

PLEASE FILL OUT THE SURVEY TO WIN A $50 GIFT CARD!

48

QUESTIONS?

Phillip Long
Business Information Solutions, Inc.
www.askbis.com
251-405-2527
plong@askbis.com

49