A WBM TECHNOLOGIES WEBINAR

Cybersecurity for your Business: Where to Begin

HOUSEKEEPING ITEMS

- Presentation will be followed by a Q&A
- To ask a question, use the Q&A Button at bottom of screen
- Recording and answers to your questions will be emailed after the event

ABOUT WBM

- Managed Services Provider located across Western Canada
- 70 Years young
- 4 key areas of expertise:
  - Managed Print
  - End User Computing
  - Enterprise Service Desk
  - Data & Security
- Clients in Diverse Industries

Your Hosts

Ilija Stankovski

Cybersecurity Expert
WBM Technologies

Ryan Lockwood

Marketing & Brand Manager
WBM Technologies

PART ONE

Definitions

Cybersecurity for your Business: Where to Begin

WHAT IS CYBER SECURITY?

- Today we associate Cyber Security or Information Security with a discipline of protecting computer systems from abuse by third parties

Disclaimer: *What I say during this webinar is not the silver bullet. There are many different solutions to a given security issue. All businesses are different, for example, some may face unique regulatory requirements that require a different approach or solution. Please keep this in mind, this webinar is for educational purposes only.*

YOU ARE HERE, SO IT MEANS YOU CARE

- You must have heard about Cyber Security attacks in the news and are worried about your business?
- You want to make sure that you remain competitive in your line of business?
- You want to use Technology as an enabler and not a detriment to your business?
- Yes, Yes and Yes … so where do I begin?

1. THREAT

- In the scope of Cyber Security threats and actors are one of the same. Marketing and media calls them “bad guys” or “cyber criminals” or “Hackers”.
- Essentially a group of people that in some way benefit from doing harm to your business.
- Examples?
  - Governments (Very difficult to protect against)
  - Real criminals (Very effective and aggressive)
  - Activists (Very specific in nature)

2. VULNERABILITY

I'll take Cybersecurity or $500, Alex … Answer: found commonly in all computer software and hardware…

- … What is, mistakes made by humans?
- Inherently ALL software and hardware will have built-in "mistakes"
- If these mistakes are used to disrupt the piece of software or hardware, that makes them VULNERABILITIES.
- Wait! I am a human. I make mistakes. Does that mean I am a vulnerability too?
- You bet, you are wetware and as vulnerable (if not more) than any software or hardware

3. EXPLOIT

- Now that we know what THREAT and VULNERABILITY means, this should be simple.

An EXPLOIT takes advantage of a VULNERABILITY when executed by a THREAT.

- Exploits can also be software, hardware or wetware (this is where the rest of the word soup continues Trojan, Virus, Spyware, Malware, Ransomware, Zero-Day, Keylogger etc.)

PART TWO

What Can You Do?

Cybersecurity for your Business: Where to Begin

MANAGE RISK

The Cyber Security industry is focused on mitigating the Risk increased through Exploitation of Vulnerabilities by Threats

- We manage Risk by implementing Controls via Standards
- Now repeat … Risk, Controls, Standards
- Again … Risk, Controls, Standards

REDUCE RISK

- Implement Controls to reduce Risk related to Cyber Security threats.
- There are three types of Controls:
  - People Controls
  - Technology Controls
  - Policy Controls
- By using Standards commonly used in the industry.

PEOPLE CONTROLS

- I start here because in majority of attacks, the exploit was a human. The wetware failed!
- Did you ever receive e-mails that ask you to click, open, view or act on a super-duper deal?
- Did you ever receive an e-mail from your CFO asking you to transfer money?
- Did you ever receive an e-mail from your Controller to change bank accounts for some equipment purchase?
- Some of our clients did and they acted on these emails!

PEOPLE CONTROLS

1. Dedicate someone to be responsible for Cybersecurity
   Make sure to hire someone that will execute work coming up in next slides and then some more
2. Enroll in End-User Awareness program … PRONTO
   This can be inhouse training, on-line training, posters, brochures, discussions in meetings, lunch'n'learn's etc…

TECHNOLOGY CONTROLS

- If Technology is part of the problem, then it also must be part of the solution
- Luckily, there is an innovative industry segment that provides technology solutions
- Here are some quick wins to get you started

TECHNOLOGY CONTROLS

- Subscribe to cloud-based E-mail advanced e-mail protection
- Implement Next Generation Firewalls with advanced security services
- Implement End-Point protection
- Backup, Backup, Backup

Legally speaking, I am not allowed to say the word "guaranteed". But I am "very confident" that if you implement these four technology controls, you will "most likely" reduce your risk significantly …. sigh … lawyers!

POLICY CONTROLS

- What is a policy Control?
  - So this is where people lose steam, because it gets a little dry
  - Policy Controls are about Governance, Documentation and Legal-Double-Speak
  - But, at the very least do this…

POLICY CONTROLS

- **Document a Security Incident Response process**
  It is just a matter of time before you are the one that is on the receiving end of a Cyber attack. Be prepared and follow a documented process that eliminates emotions like fear … and doubt.

- **Get an insurance policy**
  Make sure you have financial support when your business is disrupted. And guess what? Insurance companies like to see you take proactive steps. So you completing everything we suggested today (and more) "should help" (again lawyers) in reducing insurance premiums and support payouts when needed.

BONUS SUGGESTION

- About once per year, hire a Non-Threat that will assess your environment and find the weak spots.
- Make sure the assessment is completed by a neutral 3rd party (i.e. not your employee or IT partner).

SUMMARY

People Controls

1. Hire a Cyber-specialist
2. End-user awareness

Technology Controls

1. Get Cloud Based email protection
2. Install NGFWs
3. End-Point Protection
4. Backup, Backup, Backup

Policy Controls

1. Security Incident Response Process
2. Insurance Policy

PART THREE

Q & A

Cybersecurity for your Business: Where to Begin

A WBM TECHNOLOGIES WEBINAR

THANK YOU!

A WBM TECHNOLOGIES WEBINAR

Cybersecurity for your Business: Where to Begin


WB
WM