SO YOUR NOT-FOR-PROFIT HAS BEEN HACKED… NOW WHAT?

PRESENTED BY: BDO Canada

Thursday, OCTOBER 17, 2019

INTRODUCTIONS

STEVE M BROWN

Steve is a PMP certified Senior Project Manager with over 12 years of software project management experience. He has a solid understanding of tools and techniques for planning, organizing, monitoring and controlling IT/software delivery projects.
Steve has successfully managed technology implementations and strategic roadmap engagements and cybersecurity assessments for clients in the not-for-profit space.

As a project manager, Steve has a strong proficiency with project management tools and methodologies and is experienced with maintaining a central repository of project schedules, plans, reporting and deliverables. Steve is a determined, dynamic team player who welcomes challenging problems that require strong analytical and problem solving skills. Steve is strongly committed to total quality, continuous learning and client satisfaction.

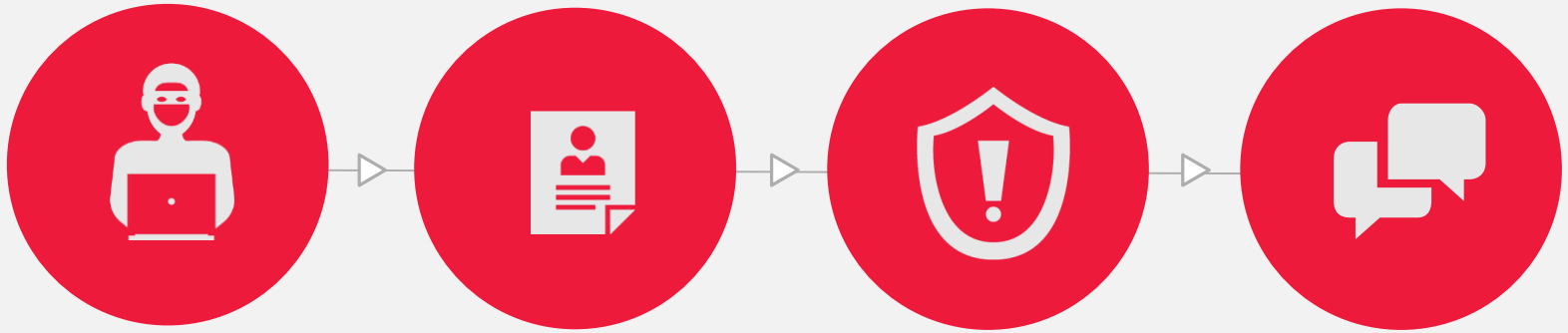
ANISHA GUPTA

Anisha is a Senior Consultant in the Cybersecurity practice with over 6 years of experience. Anisha brings experience in assessment and implementation of security standards such as ISO 27001, NIST and other privacy compliances such as GDPR and PIPEDA. She has also conducted various Application controls and IT General Controls audits.

Prior to joining BDO Canada, Anisha has worked with BDO India and other consulting firms such as PwC and EY. She has performed various cyber security assessments and evaluated third party processes delivering the client leadership gap reports for business critical processes. Anisha also holds a certification in RSA Archer and she has designed various strategies and implemented Archer offering a point click interface for helping users automate processes, streamline workflows and control user access. Anisha is also RSA Archer 5.x certified.

THE PLATFORM

AGENDA



1

Indications you've been hacked…

2

Implementation of best practices and policies

3

Preventing future cyber attacks

4

Questions

1. INDICATIONS YOU'VE BEEN HACKED…

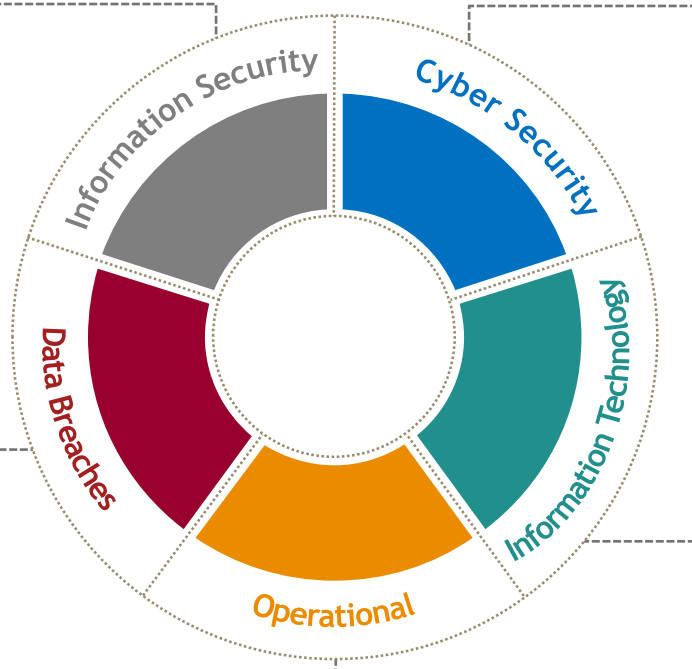
STEVE M BROWN AND ANISHA GUPTA, BDO CANADA LLP

INDICATIONS YOU'VE BEEN HACKED…

Different types of incidents

- Unauthorised/accidental disclosure of critical information
- User password compromise
- Theft/loss of equipment/documents
- Unauthorised access by first, second or third party

- Malware
- Ransomware
- Phishing Attacks
- SQL Injection Attacks
- Cross-Site Scripting
- Denial of Service Attacks
- Session Hijacks



- Breach of personal information
- Breach of data on move/during transfer
- Employee errors/negligence/improper disposal
- Physical theft

- Service tickets for fixing company assets (laptops/ workstations)
- Interruptions in network operations
- Unauthorised download of software
- Unauthorised upload/sharing of documents on personal drives

- Fire incidents
- Medical incidents
- Natural disasters
- Frauds

INDICATIONS THAT YOU HAVE BEEN HACKED

THINGS TO LOOK FOR..

MALWARE

A malware attack is an attack where a hacker inserts malware/malicious codes inside the victim's system without their knowledge. Ex: Viruses, Worms, and Trojan.

RANSOMWARE

An attack where systems are hacked and users are prevented from using their systems. Access is only regained once a ransom is paid as demanded by the hacker.

PHISHING ATTACKS

Phishing refers to use of deceptive email means to trick individuals into disclosing sensitive personal information. The hacker sends links which once clicked by the user leaks all their information.

SQL INJECTION ATTACKS

The hacker manipulated a SQL query to exploit non-validated input vulnerabilities in a database. Ex. Union Based SQL Injection.

INDICATIONS THAT YOU HAVE BEEN HACKED

THINGS TO LOOK FOR..

CROSS SITE SCRIPTING

This is commonly found in web applications. XSS enables hackers to inject their scripts into web pages used by other users allowing them to retrieve all information of the users.

DENIAL OF SERVICE ATTACKS

Attacks where services are made unavailable to the intended users by penetrating/ intruding into the network and disrupting the host connected to the internet.

SESSION HACKS

Attacks interrupting operations due to exploitation of a computer session to gain unauthorized access to systems. This is also called Cookie Hijacking.

PASSWORD ATTACKS

Attacks such as Brute Force attacks where the hackers try to crack passwords to penetrate into the organization's network/systems.

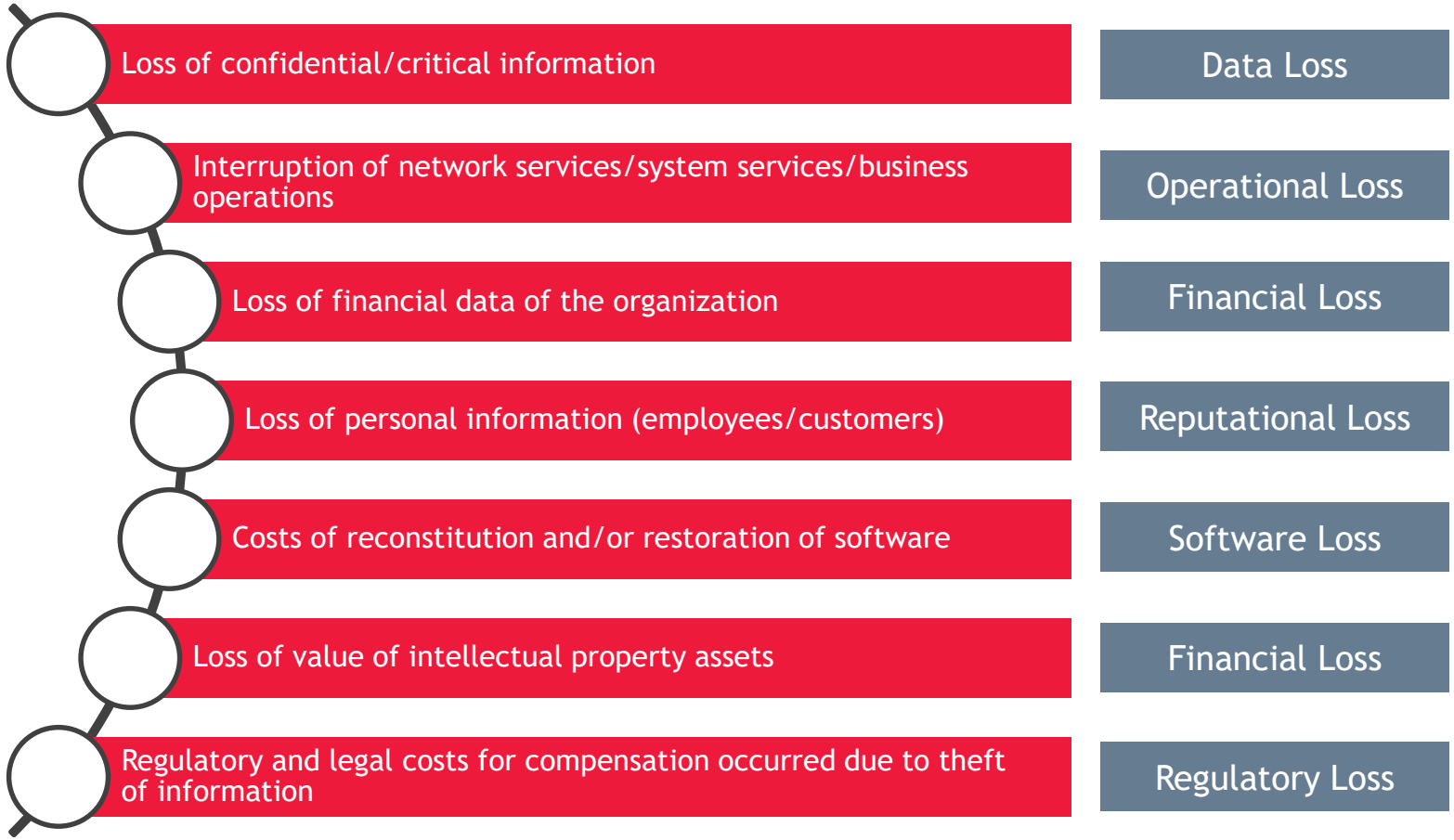
INDICATIONS THAT YOU HAVE BEEN HACKED

THINGS TO LOOK FOR..

FREQUENT AND RANDOM POP-UP WINDOWS	AUTO-REDIRECT	MOVING MOUSE PONTER	ANTI-VIRUS SHUTTING DOWN	FREQUENT CRASHES	RANSOMWARE MESSAGE
▶ When you receive pop-ups on websites that usually don't show them.	▶ When browser automatically redirects user to random and unwanted websites without user's permission.	▶ The mouse pointer randomly moves by itself.	▶ Abnormal shut down of anti-virus program. Often users experience difficulty in re-enabling anti-virus program.	▶ Unusual slow computer performance.	▶ Screen take-over by hackers asking user to pay for lost data.

INDICATIONS THAT YOU HAVE BEEN HACKED

Impacts of an incident



INDICATIONS THAT YOU HAVE BEEN HACKED

Determination of what type of data has been breached

CRITICAL/CONFIDENTIAL INFORMATION (INTELLECTUAL PROPERTY):

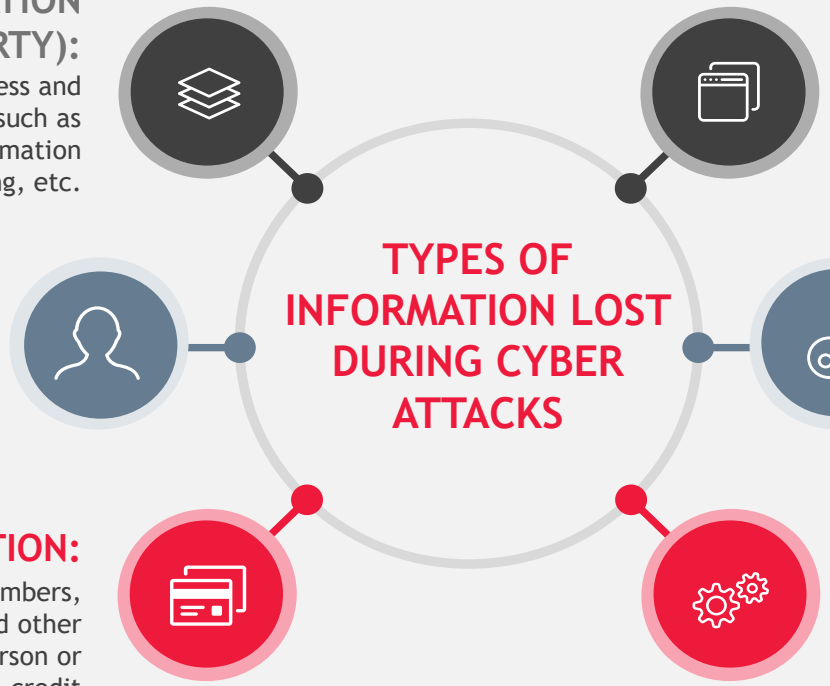
Any Information which needs authorized access and cannot be shared outside the organization such as trade secrets, technology information, information pertaining to customers, pricing and marketing, etc.

PERSONAL INFORMATION:

Personally identifiable information such as name, age, address, bank account details and much more, of not only employees, but also customers of the organization

FINANCIAL INFORMATION:

Information such as credit card numbers, credit ratings, account balances, and other monetary facts about a person or organization that are used in billing, credit assessment, loan transactions, and other financial activities.



ORGANIZATION INFORMATION:

Information about business operations and business strategies set by the organization which is not subject to public interest

CREDENTIALS:

Passwords and usernames of all network devices, database systems, assets (laptops/ workstations), mobile devices, and other access controlled devices in the organization

SYSTEM CONFIGURATION INFORMATION:

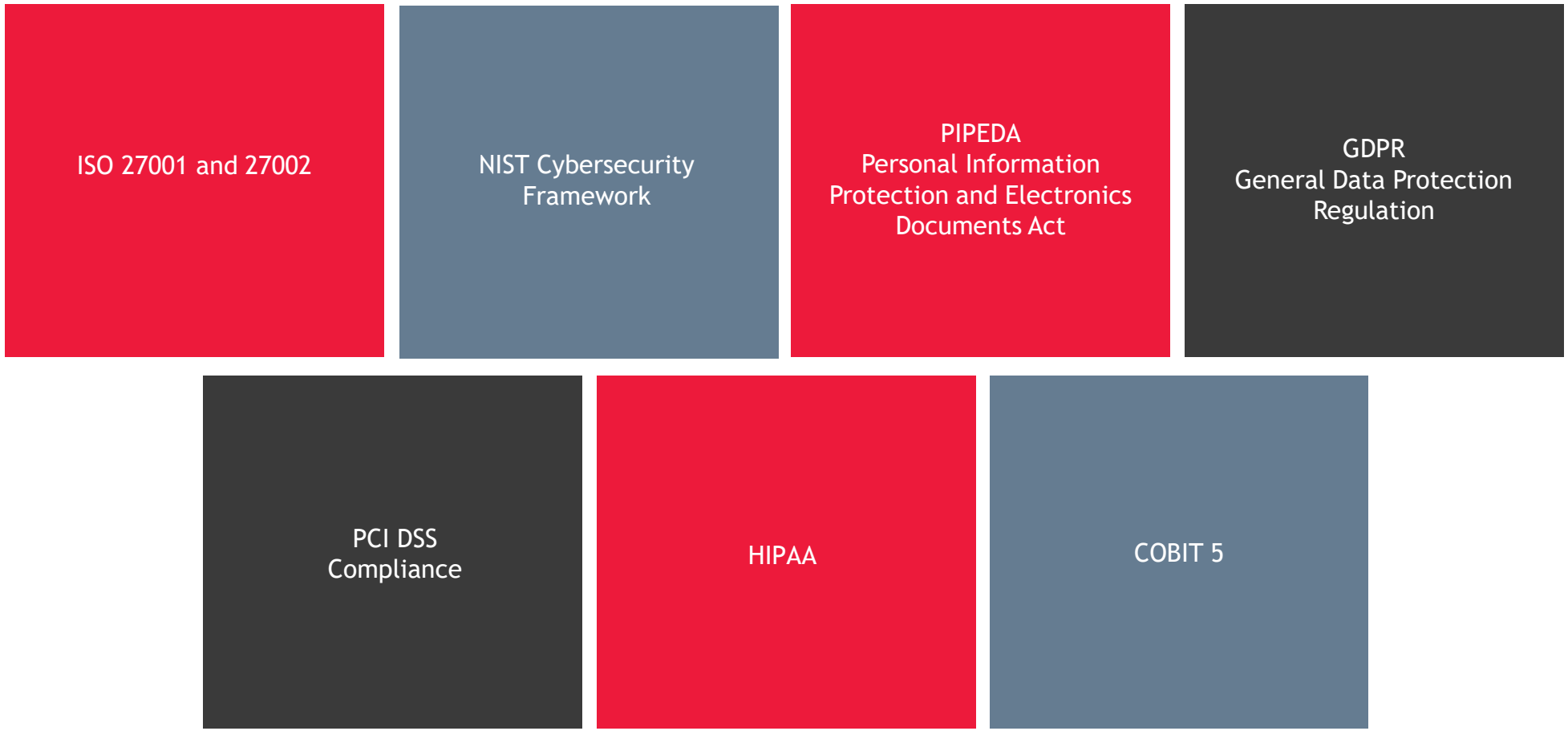
Configuration details of all network related devices which are shared among the authorized individuals within the organization

2. IMPLEMENTATION OF BEST PRACTICES AND POLICIES

STEVE M BROWN AND ANISHA GUPTA, BDO CANADA LLP

IMPLEMENTATION OF BEST PRACTICES AND POLICIES

INDUSTRY'S BEST SECURITY STANDARDS AND PRACTICES



IMPLEMENTATION OF BEST PRACTICES AND POLICIES

Risk/Cyber Security Assessment

A cyber security assessment provides an in-depth review of the current security controls in the organization along with their maturity to mitigate the potential risks. Following are the major focus areas that are covered as a part of the assessment:

INTERNAL SECURITY ASSESSMENT

Measuring the current maturity levels of security controls in the organization and benchmarking them against industry's best security standards. Example: ISO 27001:2013, NIST etc.

VENDOR RISK MANAGEMENT

Security assessment of third parties providing services to an organization

BCP AND DISASTER RECOVERY PROCESS:

To ensure prevention from an unfavourable incident and strategies around recovery from unforeseen disasters

APPLICATION/DATABASE SECURITY ASSESSMENT:

Assessment of app controls and database controls for identification of vulnerabilities

PHYSICAL AND ENVIRONMENT SECURITY ASSESSMENT:

Evaluating physical access controls, safety mechanisms and other environmental controls

NETWORK SECURITY ASSESSMENT:

Assessment of network controls including network flow, network traffic, anti-malware controls and wireless controls

IMPLEMENTATION OF BEST PRACTICES AND POLICIES

Risk/Cyber Security Assessment

End result of an assessment

SECURITY ANALYSIS RESULT	ROADMAP FOR IMPROVEMENT	PERTAINING RISKS AND IMPACT	PREVENTIVE MEASURES
▶ Identification of Security gaps (threats and vulnerabilities) ▶ Compliance ratio	▶ Identification of security controls that need improvement ▶ Introduction of new Security controls	▶ Residual risks and their impact ▶ Inherent risks and their impact	▶ Recommendations to prevent potential threats ▶ Recommendations for mitigation of risks
Current Maturity Levels	Secure Framework	Mitigation of risks	Security enhancements

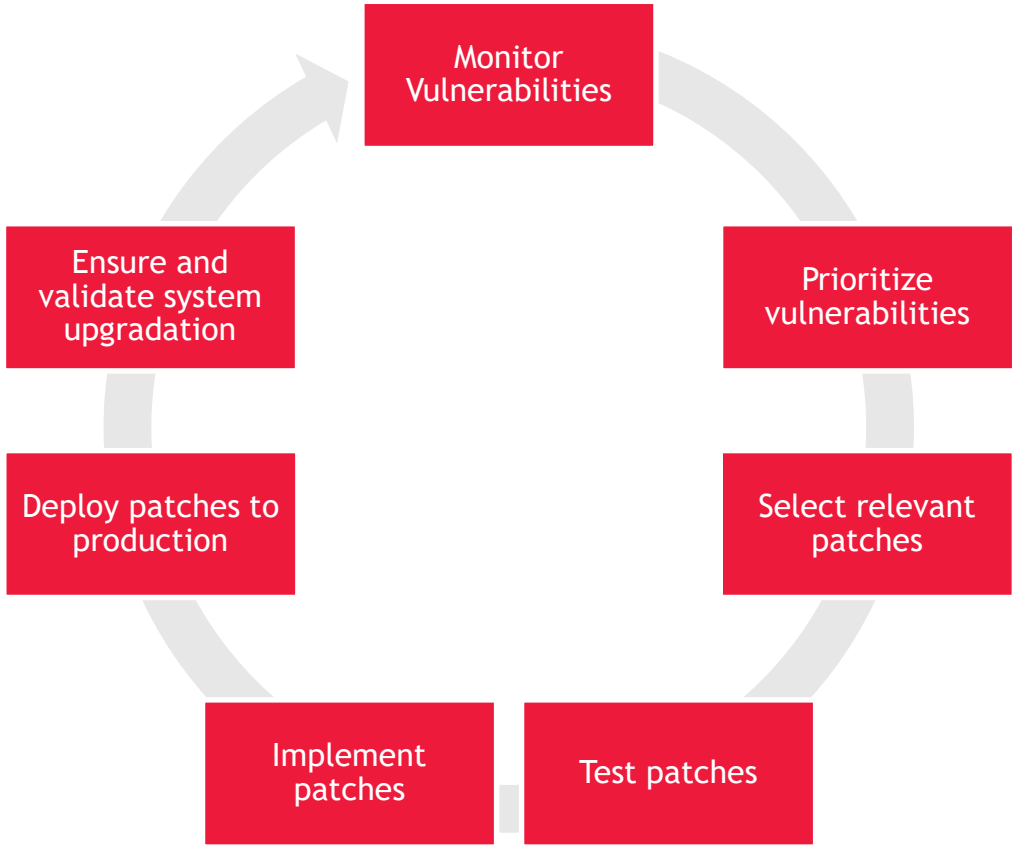
3. PREVENTING FUTURE CYBER ATTACKS

STEVE M BROWN AND ANISHA GUPTA, BDO CANADA LLP

PREVENTING FUTURE CYBER ATTACKS

System Upgrade

It is necessary to keep all systems carrying confidential information upgraded with the latest patches to avoid introduction of various vulnerabilities. Increase in vulnerabilities lead to increase in potential threats resulting in cyber attacks. Following is the process that should be followed for patch and vulnerability management to avoid unforeseen incidents:



PREVENTING FUTURE CYBER ATTACKS

Being more ready/being more proactive & focus spending on protecting key areas

How to mitigate risks for potential threats?

PERIODIC ASSESSMENTS OF CURRENT SECURITY CONTROLS

Regular audits/ assessments to be conducted to improve current security framework/posture

REAL TIME MONITORING/ PROCESSES/ TOOLS

Tools implemented to monitor and alert incidents on real time basis. Example: SIEM. This helps organizations respond to incidents in minimum time and results in minimum damage to the organization

DETECTIVE AND PREVENTIVE MEASURES

Policies and processes defined around detective and preventive measures for analysing and containing the incidents

RESPONSE STRATEGIES

Response strategies are designed to help the teams gain preparedness to potential incidents. It helps organization develop necessary capabilities to handle incidents/breaches

RISK ASSESSMENT PROGRAMS

Risk Assessment should be performed keeping in mind all critical business processes and assets to ensure that there are necessary security controls that have been implemented to safeguard the critical information being held by the organization

PREVENTING FUTURE CYBER ATTACKS

Security Awareness for employees

- Develop information security awareness trainings for incident reporting
- Ensure every new/current employee has undergone the security awareness trainings
- Perform incident awareness tests to ensure all individuals in the organization perform their actions with efficiency
- Develop a call tree to allocate responsibilities to stakeholders who shall be contacted during an incident
- Create posters, flyers, screensavers and other awareness material to market the importance of incident reporting
- Communicate incident management policy and procedure to all employees along with a list of Do's and Don'ts

4. QUESTIONS?

CONTACT INFORMATION

STEVE M BROWN
BDO Canada LLP
Senior Project Manager

smbrown@bdo.ca
416- 895- 1617

ANISHA GUPTA
BDO Canada LLP
Senior Consultant

vgupta@bdo.ca
647- 258- 9467

BDO GLOBAL STATISTICS 2018

GLOBAL REVENUE

US$9 BILLION

10.7%
Increase over 2017

162
countries & territories

1,591 offices

up by **6%**

GLOBAL HEADCOUNT

80,087

8.4%
Increase year on year

GLOBAL AVERAGE PROFESSIONAL PARTNER TO STAFF RATIO

1 TO 10