Cyber Security

Presenters:
- Brian Everest, Chief Technology Officer, Starport Managed Services
- Susan Pawelek, Accountant, Compliance and Registrant Regulation

February 13, 2018 (webinar)
February 15, 2018 (in-person)

OSC ONTARIO SECURITIES COMMISSION

Disclaimer

The views expressed in this presentation are the personal views of the presenting staff and do not necessarily represent the views of the Ontario Securities Commission or any of its other staff.

The presentation is provided for general information purposes only and does not constitute legal or accounting advice.

Information has been summarized and paraphrased for presentation purposes and the examples have been provided for illustration purposes only.

Information in this presentation reflects securities legislation and other relevant standards that are in effect as of the date of the presentation.

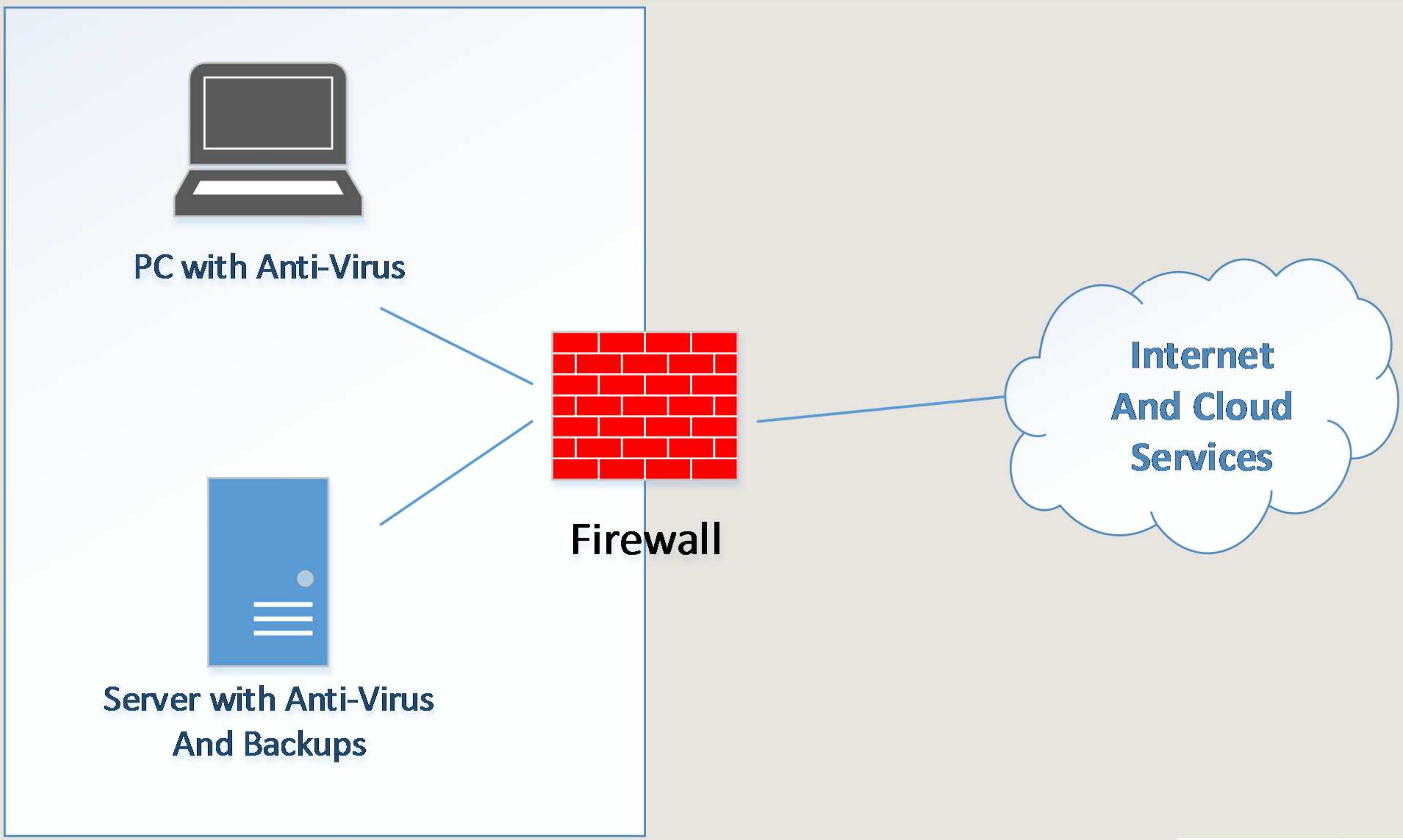
The contents of this presentation should not be modified without the express written permission of the presenters.

Agenda

- Cyber Security – the Basics
- New Kinds of Risks and Threats
- Overview of Staff Notice
- What Can You Do? – #1 The Basics
- What Can You Do? – #2 Defense in Depth
- Summary

Cyber Security
The Basics

Typical IT Environment



IT Security Basics

- Firewalls
- Anti-Virus
- Windows Patching
- E-mail and Spam Filtering
- Monitoring and Logging
- IT Policies and Procedure
- Backup and Disaster Recovery

Common IT Threats

- Malware – Viruses, Ransomware, Cryptolocker
- Phishing e-mails
- Social Engineering (Fraud)
- User Risk – accidental and intentional activities

New Kinds of Risks and Threats

New Kinds of Threats

- Spear Phishing (Targeted Attacks)
- Denial of Service Attacks
- Worms – like WannaCry – rapidly spreads to all vulnerable devices
- Infrastructure Vulnerabilities (Meltdown/Spectre)

New Kinds of Threats

- Spear Phishing (Targeted Attacks)

New Kinds of Threats

- Denial of Service Attacks
  - Both network attacks and internal IT services can be targeted
  - Nayana, a web hosting company, paid $1M ransom to stop a DDoS
- DDoS attacks can also be used as cover for other hacking activities – they can be used as a distraction for IT staff

New Kinds of Threats

- New Types of Malware
- Worms – like WannaCry – rapidly spreads to all vulnerable devices
- CryptoMining viruses that generate revenue
- Fileless Malware that is not detectable by regular anti-virus

New Kinds of Threats

- Infrastructure Vulnerabilities (Meltdown/Spectre)

Changes to Cyber Threats - Hackers

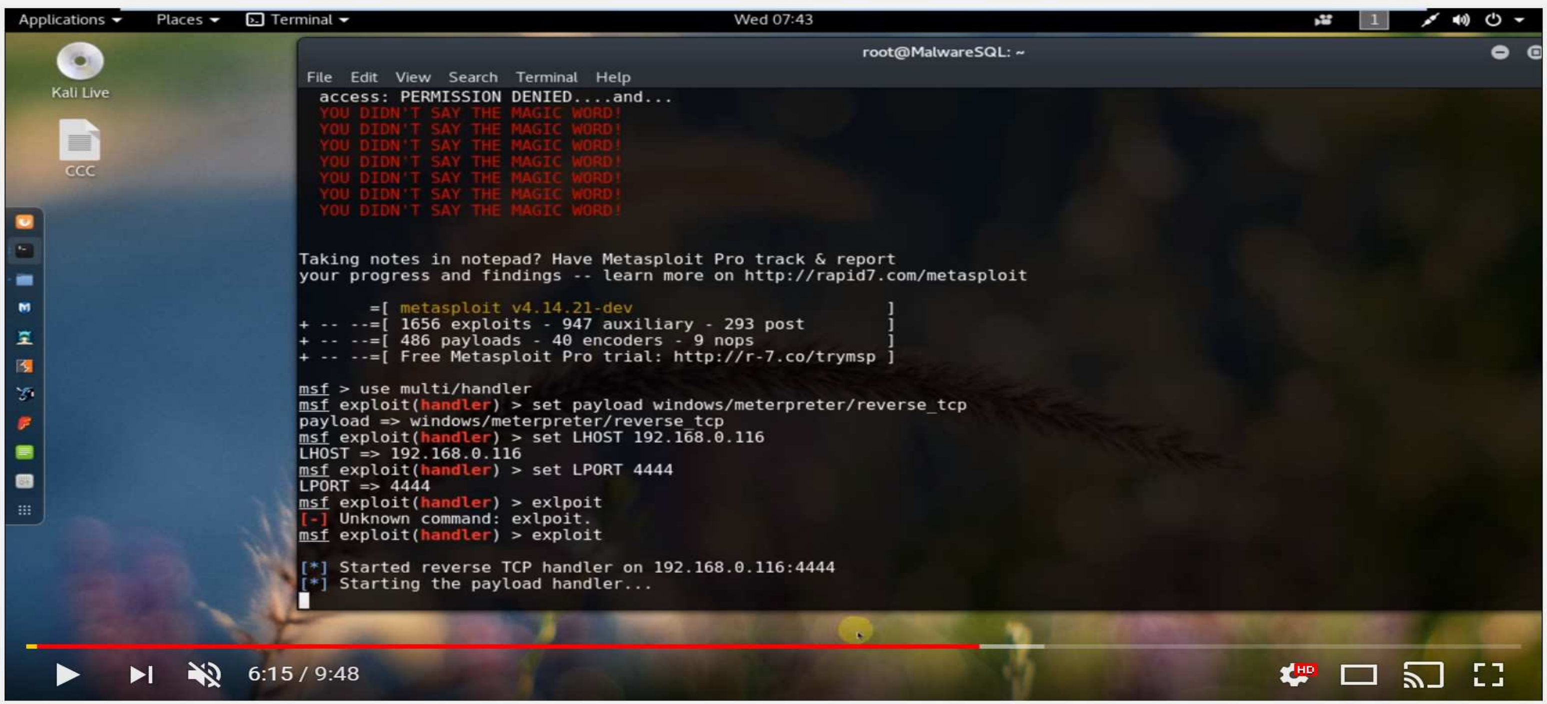
- Many threats are now targeted and profit driven
- Organized crime involved using paid IT staff
- Hacking organizations like Anonymous and Shadow Brokers
- Government sponsored attacks

Hacker Behaviour

- Often delays of days or weeks from initial installation of spyware to the breach of data
- Network hacks can be sold – someone can pool together data, botnets or compromised sites and sell access to a 3rd party
- Average Cyber Criminal age is now 17 and may be working as a contractor

Hacking for Dummies

Free toolkits available for launching attacks



Hack Windows 10/8/8.1/7 With Metasploit || Kali Linux 2017.1

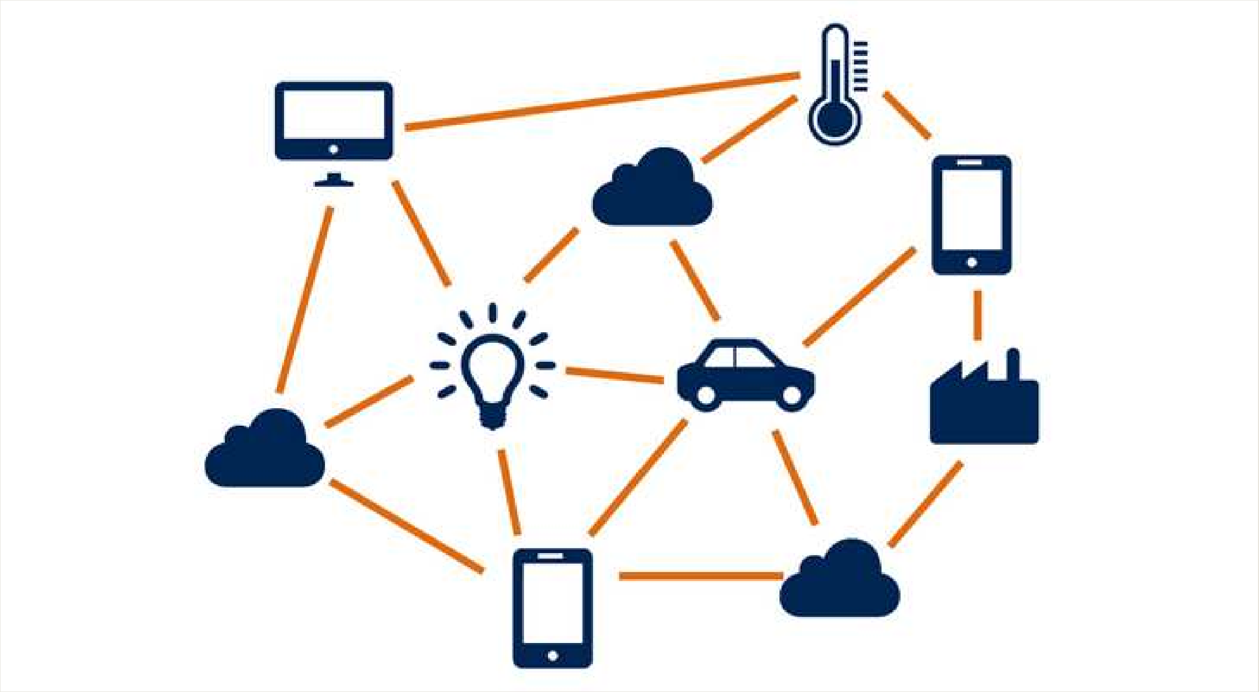
starport MANAGED SERVICES

Social Media

- Combining information from social networks (Twitter, Facebook, LinkedIn) with real world information (official websites, phones lists) to perform social engineering attacks

IoT (Internet of Things)

Interconnectivity of devices poses new risks



Favourite Hacker Targets

- Crypto Currency Exchanges – perfect storm of high value targets in new markets with new IT infrastructures

Exchange	Year of Hack	Value ($CDN)	Currency
Bitcoinica	2012	$7M	Bitcoin
Mt Gox	2014	$490M	Bitcoin
NiceHash	2016	$92M	Bitcoin
Veritaseum	2017	$11M	Ethereum
Coincheck	2018	$650M	NEM
	Total	$1.2B	

Overview of Staff Notice 33-321 *Cyber Security*

Overview of NI 33-321

Published On October 19, 2017

Includes:

- Results of survey sent in 2016
- Guidance
- Expectations for CSA registered firms

Components of cyber security preparedness

Main components of a firm's cyber security preparedness:

1. Policies and procedures
2. Training
3. Incident response plan

1. Polices and procedures

Policies and procedures should include the following:

- Use of electronic communications
- Use of firm-issued electronic devices
- Loss or disposal of an electronic device
- Use of public electronic devices or public internet connections
- Detecting internal or external unauthorized activity
- Ensuring software is updated in a timely manner
- Overseeing third-party vendors / service providers
- Reporting cyber incidents

Risk Assessments

What to include in a risk assessment:

- Inventory of the firm's critical assets and confidential data
- Vulnerable areas of the firm's operations
- How cyber threats and vulnerabilities are identified
- Potential consequences of cyber threats identified
- Adequacy of preventative controls

2. Training

Employees often first line of defence

Training should include:

- Risks associated with the data collected, used or disclosed
- Safe use of electronic devices

Training should take place with sufficient frequency to remain current.

3. Incident response plan

A written incident response plan should include:

- Who should be involved in communicating about the incident and responding to the incident
- Different types of cyber attacks the firm might face
- Procedures to stop / neutralize the threat
- Procedures to recover data
- Identification of parties that should be notified

Outside service providers

a) Due diligence
   - Evaluation of service provider's cyber security
   - Limit access to firm's systems and data

b) Written agreements
   - Include provisions related to cyber threats

c) Cloud services
   - Security practices of cloud service provider

Other

Insurance

Data protection:

- Use of encryption
- Strength of passwords

What Can You Do?

#1 - Cover the Basics

Expert IT Security Advice

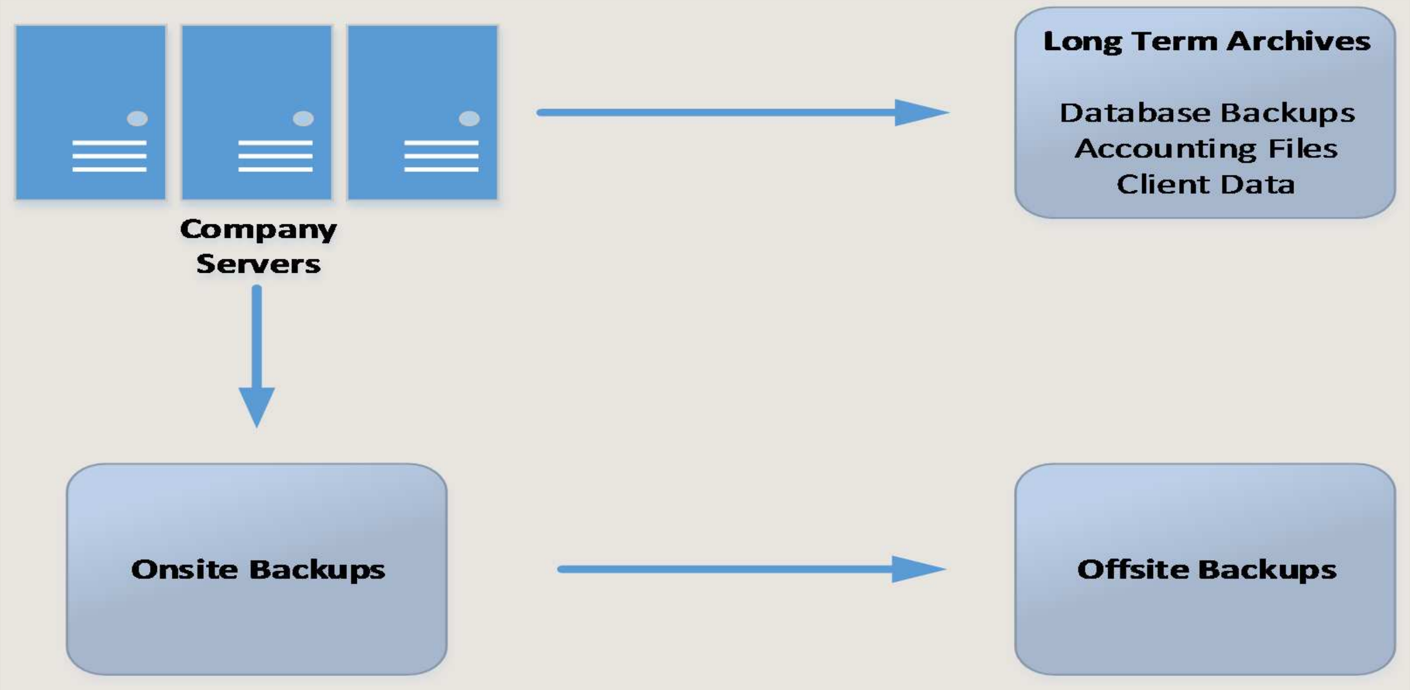
- Assessing risk requires an understanding of your business requirements and knowledge of current IT threats
- Consult with Security Experts about the right solutions for your business – whether your in-house IT group / security division or with a 3rd party
- Regularly review security best practices – Cyber Security is the fastest growing area in IT for both new threats and new solutions

Preventative IT Maintenance

- Windows Patches tested and applied in a timely manner
- Automating windows patching and anti-virus updates
- Central monitoring of all the patching – so someone is reviewing the updates and addressing problem servers or PCs
- Update switches and firewalls firmware

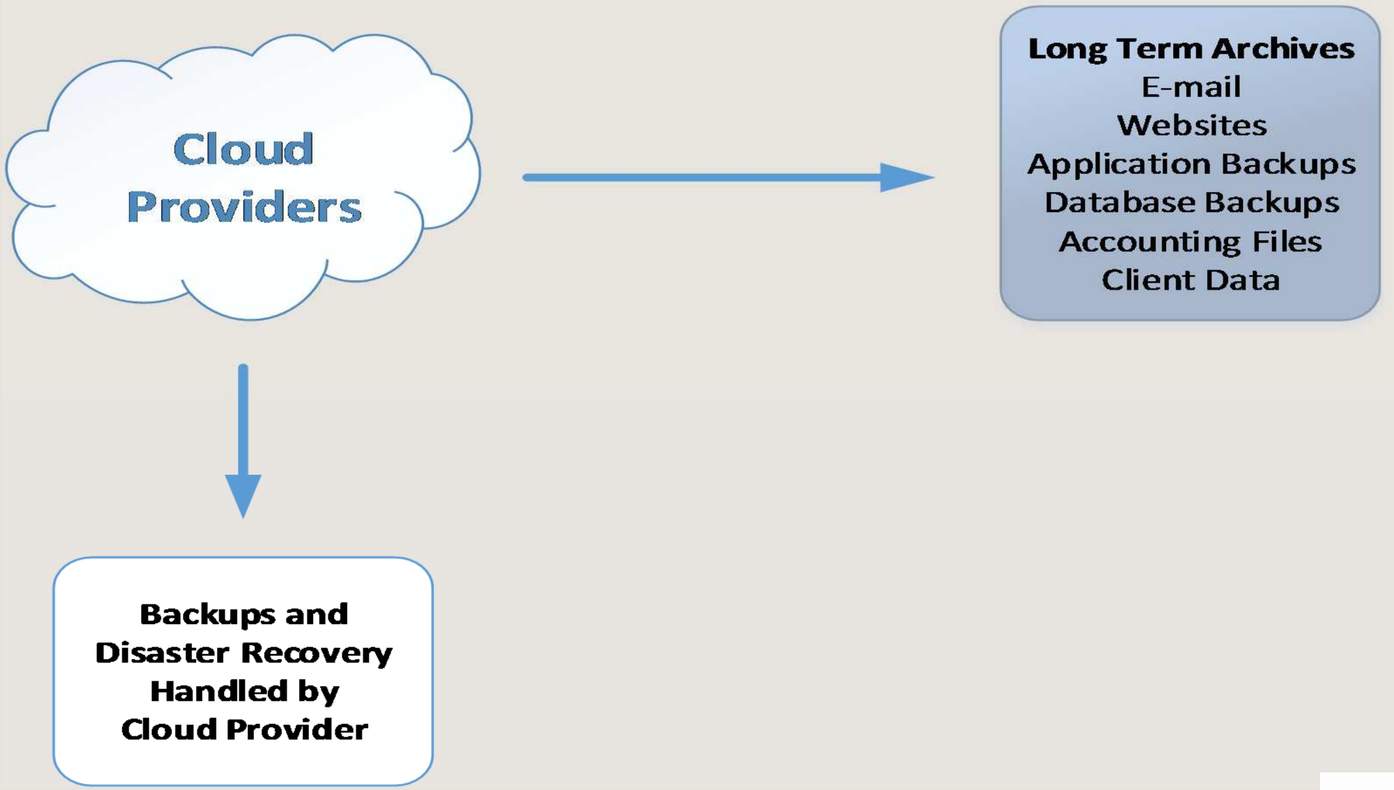
Backups and Archives

- Backups are a key element in recovering from Cyber incidents
- Should be at least 3 separate locations for backups – onsite, offsite and long term archives



Using the Cloud

- Companies trust their cloud providers to handle backups and disaster recovery
- Recommend an extra layer of backup, outside of the cloud, not accessible by the provider



Disaster Recovery

- Incident Response Plans and Disaster Recovery Scenarios need to include Cyber issues
- Disaster Recovery has to be the last line of defense against Cyber Security Threats
- Server images with “instant recovery” and Cloud Provider with immediate failover should be used

Monitoring IT

- Malware and social engineering attacks usually take place inside your network
- Your current IT infrastructure may not have visibility into what is going on until it impacts your business
- The challenge is to monitor IT in real-time and be alerted for suspicious activity as it is happening

IT Security Responsibilities

What a Firm's IT infrastructure does

vs.

What Users have to do to be secure

Social Engineering

- Social Engineering is becoming as important as technical tools for attacks

AND

- Security Awareness Training is just as important as technical tools for defense

Secure Passwords

- Pass phrases can work better (brownbasketfour) then complex passwords (P@ssW0rD)
- Ultimate combination is a password that uses lower and uppercase, numbers and special characters and is at least 12 characters
- Preferable not to rely on only usernames and passwords for authentication

Authentication Best Practices

- Preferable not to rely on only usernames and passwords for authentication
- Use 2 factor authentication whenever it is available
- Respond to any alerts about failed login attempts
- Use different passwords for different services

User Response to IT Threats

- Use a second channel for approvals for e-mail requests to prevent Spear Phishing attack from succeeding.
- Delete suspected e-mail without opening and confirm with the sender if the e-mail was legitimate
- If there is unusual activity on your PC that you cannot stop then shutdown your PC immediately and notify IT support

Mobile Devices

Things you can do to protect your company (and yourself):

- Secure Passwords and Screen Timeout Locks
- Encrypt storage on your devices
- Don't download insecure applications
- Run management software to protect and monitor devices that connect to the corporate network and critical mobile applications

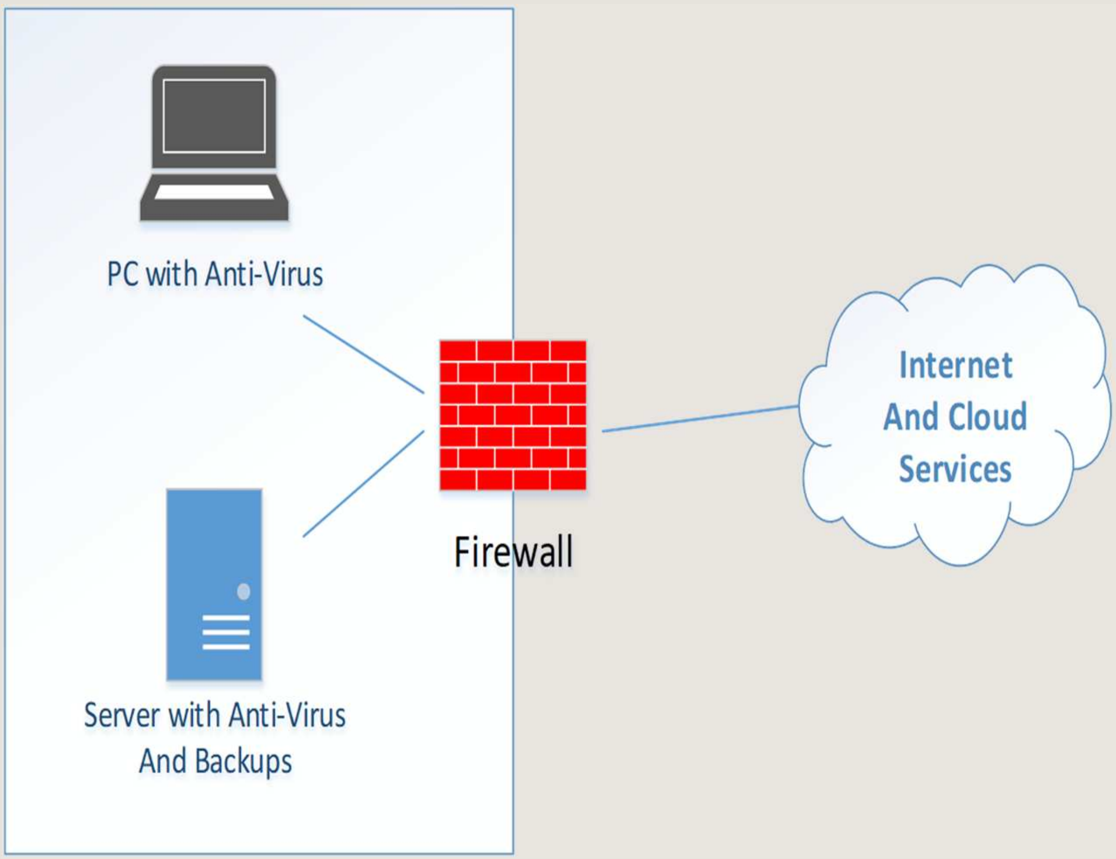
Personal IT

- Same rules apply about IT security for home equipment
- Change the default passwords on any home IT equipment (Smart TVs, wireless access points)
- Put passwords on phones, tablets and notebooks

What Can You Do?

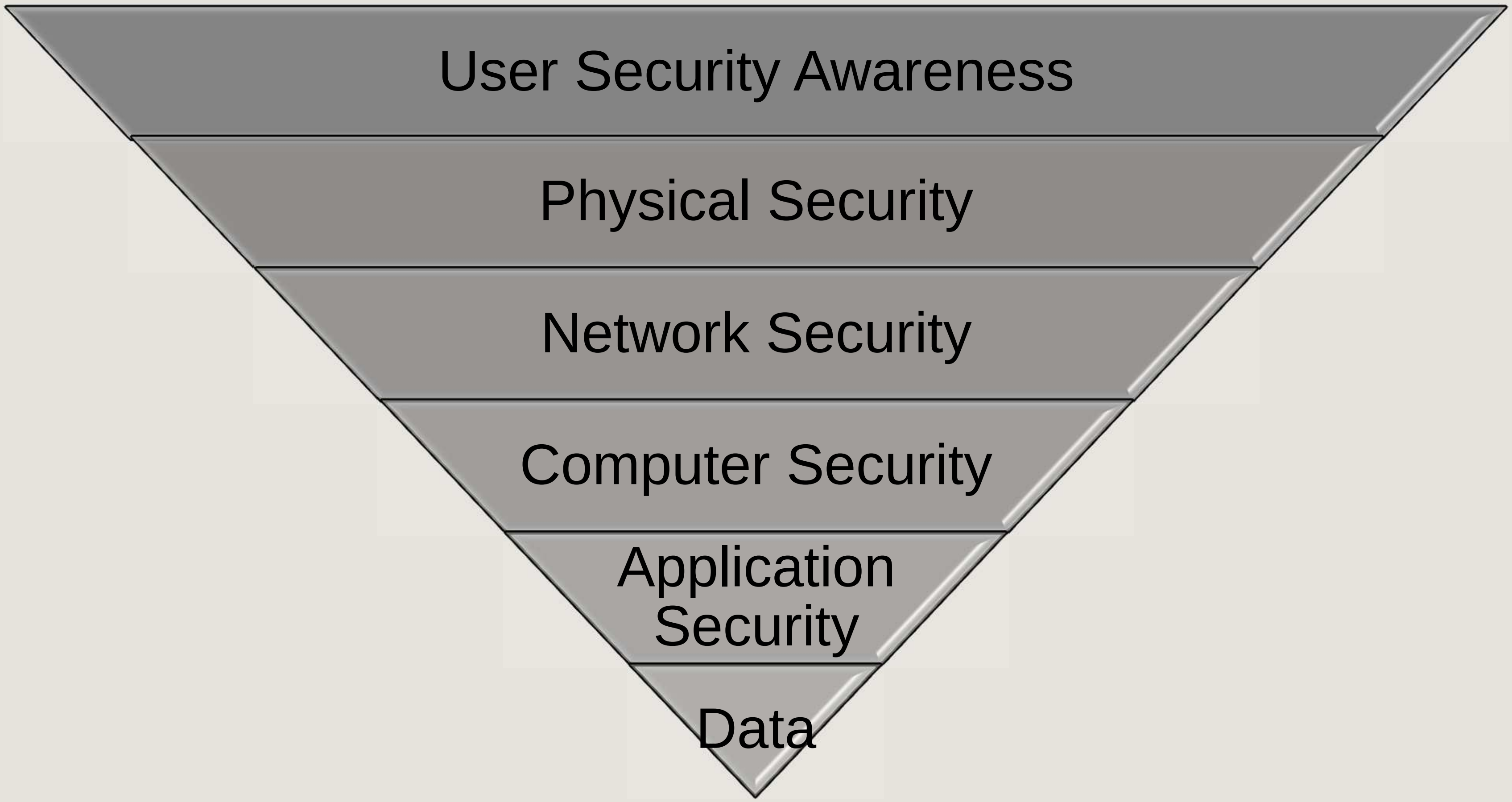
#2 – Defense in Depth

Defense in Depth

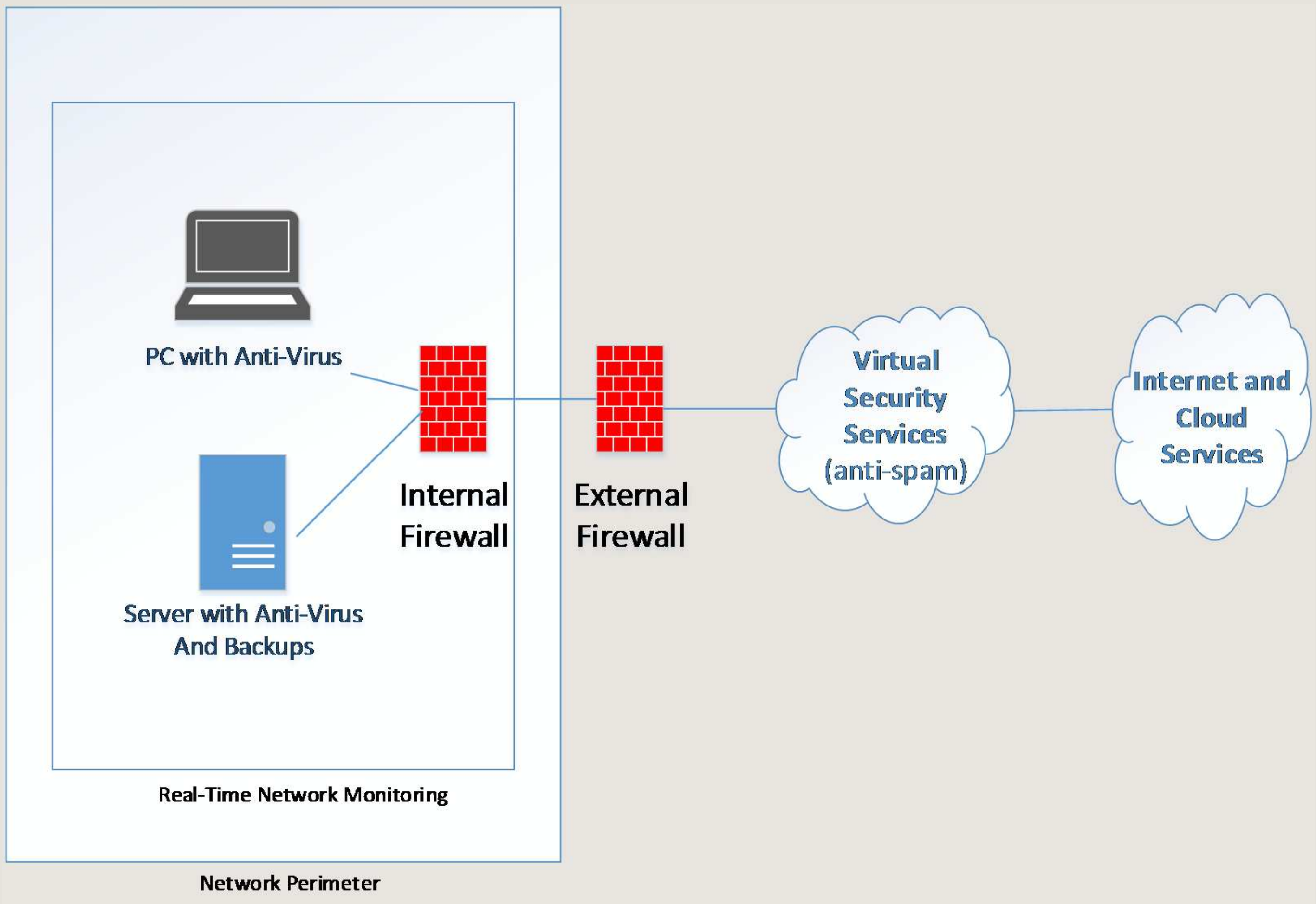


Revisiting the Standard IT Setup

Defense in Depth



Defense in Depth



Take Aways

- A Solid IT Infrastructure is the foundation of being able to handle Cyber events
- Defense in Depth – layers of IT protection is critical to mitigate cyber security issues
- Cyber Security is evolving and IT best practices need to be modified to keep up

Questions

RegistrantOutreach@osc.gov.on.ca

Contact Centre:

inquiries@osc.gov.on.ca

416-593-8314 or

1-877-785-1555 (toll free)