KPMG

Cybersecurity Risk

CAGFO Conference – September 2018

With you today

Scott MacLennan

CISSP, CISA

Senior Manager, Risk Consulting

Winnipeg, MB

smaclennan@kpmg.ca

204 957 2203

Marcus Jungbauer

CISSP-ISSAP, CISA, CCSP

Manager, Risk Consulting

Winnipeg, MB

mjungbauer@kpmg.ca

204 957 2230

Topics for today

- **Current Cyber Security Landscape**
- **Why is Phishing still an issue?**
- **Cyber Security skills shortage**
- **Risks with respect to the Internet of Things (IoT & IIoT)**
- **The latest cyber risks and attacks KPMG has seen**

Some current statistics for 2017 and 2018

- **Survey #1 conducted at end of 2017 had 33% of the respondents indicating that some form of cyber breach occurred**
  - On average takes 200 days to detect and recover from a breach
  - 60% reported malware as the root cause of the incidents

- **Survey #2 found that 35% of IT execs thought they were the biggest risk**

- **Survey #3 found that 49% of organizations rank the largest obstacle to an organization's cyber posture as a lack of skilled personnel**
  - Next was budget, security awareness and vaguely defined processes and process owners
  - The respondents stated that currently Cyber Security is approximately 15% of overall IT budget

Some current statistics for 2017 and 2018

- **Survey #2 found that attacks increased by 17% but records breached decreased by 82%**

- **Survey #3 found that 44% of organizations stated they recovered from attacks within hours and 25% within one day**

- **Also that 44% of organizations monitored their ERP systems monthly and 25% continuously**

Canadian Cyber Breaches in 2017 and 2018

- **Bank of Montreal**
- **Simplii Financial (CIBC)**
- **National Bank of Canada**
- **Equifax**
- **City of Guelph**
- **Ministry of Health (BC)**
- **Ontario Progressive Conservative Party**
- **Canada Immigration**
- **Hudson Bay Company**
- **WestJet**
- **Bell**
- **Canoe.ca (Sun Media)**
- **Nissan**
- **McDonalds Canada**
- **Canadian Tire**

Canadians are being hacked more than ever…

- **Canada Ranks 3rd in reported global data breaches**
- **One-in-five breaches are classified as "high-impact", where sensitive information was exposed**
- **Average time for Canadian companies to identify a breach increased to 181 days from 173 days last year**
- **Average time for Canadian companies to contain the data breach increased to 69 days up from 60 days last year**
- **From identification to containment is roughly 250 days on average**

Data Breach Costs in 2018

- Canada has the highest direct cost at $81 (USD) per compromised record.
- These costs are mostly related to engaging forensic experts, hiring a law firm, or offering victims identity protection services.

Average global total cost of a data breach: $3.86M (USD)

Up 6.4% from 2017

Average global total cost per lost or stolen record: $148 (USD)

Up 4.8% from 2017

A breach of 1 million records yields an average total cost of $40 million (USD)

A breach of 50 million records yields an average total cost of $350 million (USD)

Why PHISHING is still an issue?

Why is Phishing still an issue?

- **A Phishing attack is emails that are sent to get some someone to have a specific response, such as providing their passwords, clicking on a link, or initiating a money transfer**
- **In 2016 an Australian aircraft parts company lost $54 million due to a Phishing attack**
- **A January 2018 report states that 67% of businesses saw some form of Phishing attack in 2017**

What is Spear Phishing

- **Spear Phishing is more specific to the target (your organization)**
  - Attackers are using social media to create personalized directed attacks
  - Can appear to come from your organization or ARE from your organization
  - Uses specific names for realism, name of CEO, CFO, etc.

Other forms of Phishing

- **Part of the newest attack is called Smishing for SMS Phishing (Phishing via text messaging)**
  - A messaging telling you that your service provider cannot process your payment and your service will be turned off unless you enter your personal information
- **Adults 55+ recognize phishing more than Millennials**
- **Phishing attacks exploit an organization's lack of security awareness**
- **Continuous security awareness training is the key!**

Phishing

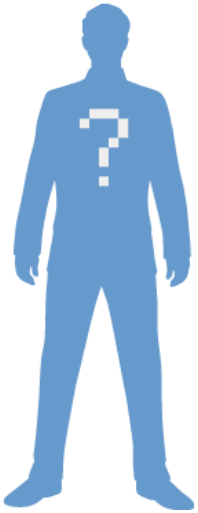
What should you do?

- **Perform security awareness training:**
  - Educate users that the most successful phishing attacks are disguised as something an employee was expecting
  - Only open “safer” attachments (PDF, DOC, XLS, PPT)
    - The EXE, VBS, ZIP, PS files are likely malicious…
  - Look for grammatical errors and re-read the FROM fields
    - **@company.co** looks very similar to **@company.ca**
  - Avoid clicking on links. Go to Google and find the site from there
  - Legitimate companies normally do not sent out threatening emails
  - If it seems suspicious it probably is! Send it to IT for review
- **Perform simulated Phishing testing to evaluate how your training program is operating**
- **Look at aggressive white/black listing for your spam filters**

Cyber SKILLS Shortage

Cyber security skills shortage

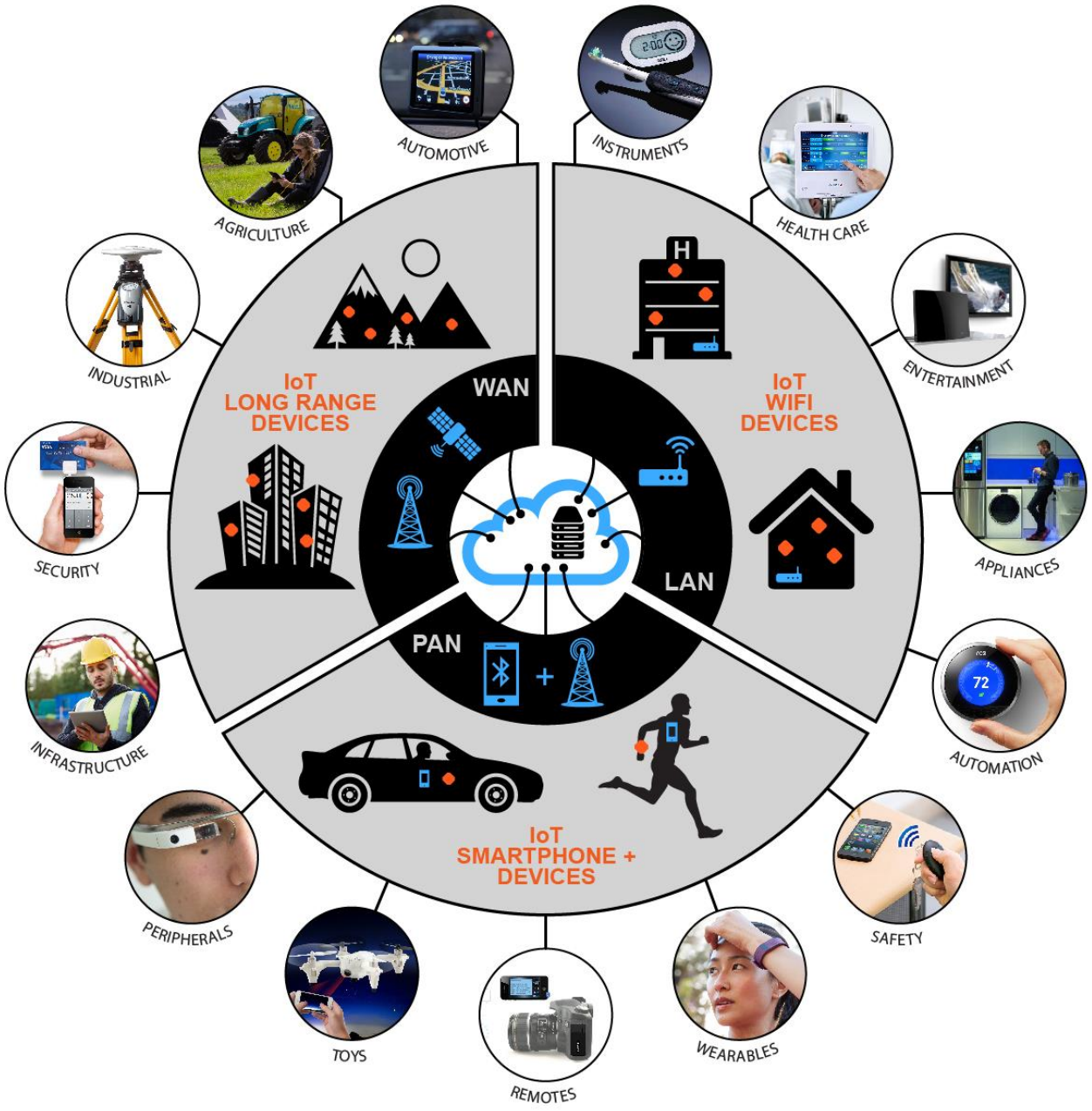
- **Most organizations are facing a cyber security skills shortage. In a 2017 survey:**
  - 54% of the respondents stated that they are planning to train or certify existing staff
  - 41% were going to partner with a managed services provider
  - 32% were going to hire additional security staff
- **The outlook for 2019 isn't looking any better…**



Cyber security skills shortage

- **One way to partially mitigate this shortage is to outsource your security resources**
- **Outsource your larger security workloads like Security Monitoring, Vulnerability Testing, Cyber Attack Simulations, Phishing Campaigns, etc.**
- **Account for third-party relationships with suppliers, partners, and external vendors (…those “Cloud” people)**
- **Have independent experts assist with Cyber Security Maturity and Risk Assessments**

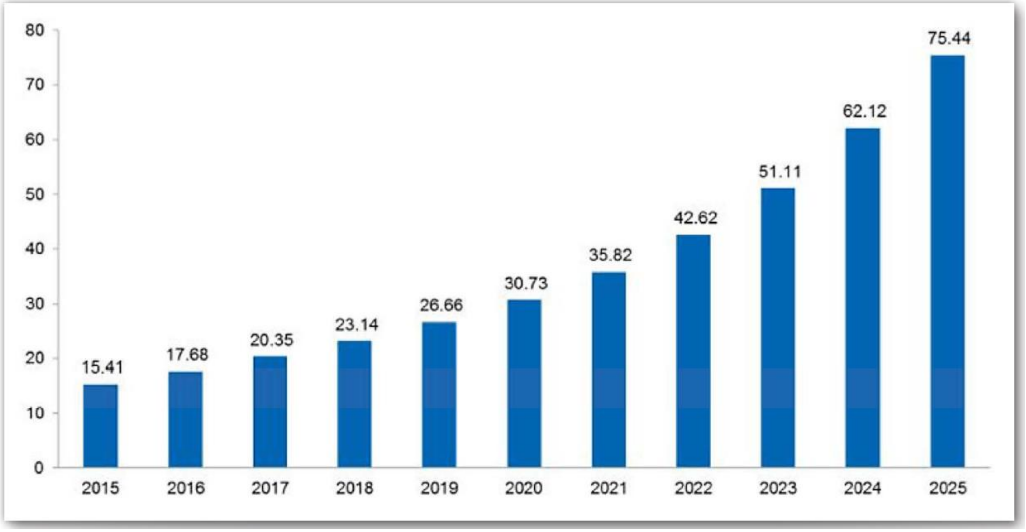
Cyber Risks for Internet of Things


AUTOMOTIVE
INSTRUMENTS
AGRICULTURE
HEALTH CARE
INDUSTRIAL
ENTERTAINMENT
IoT
LONG RANGE
DEVICES
WAN
IoT
WIFI
DEVICES
LAN
SECURITY
APPLIANCES
PAN
INFRASTRUCTURE
AUTOMATION
IoT
SMARTPHONE +
DEVICES
PERIPHERALS
SAFETY
TOYS
REMOTES
WEARABLES

Risks with respect to the Internet of Things (IoT)

- **IoT refers to refers to "physical objects that have embedded network and computing elements and communicate with other objects over a network"**

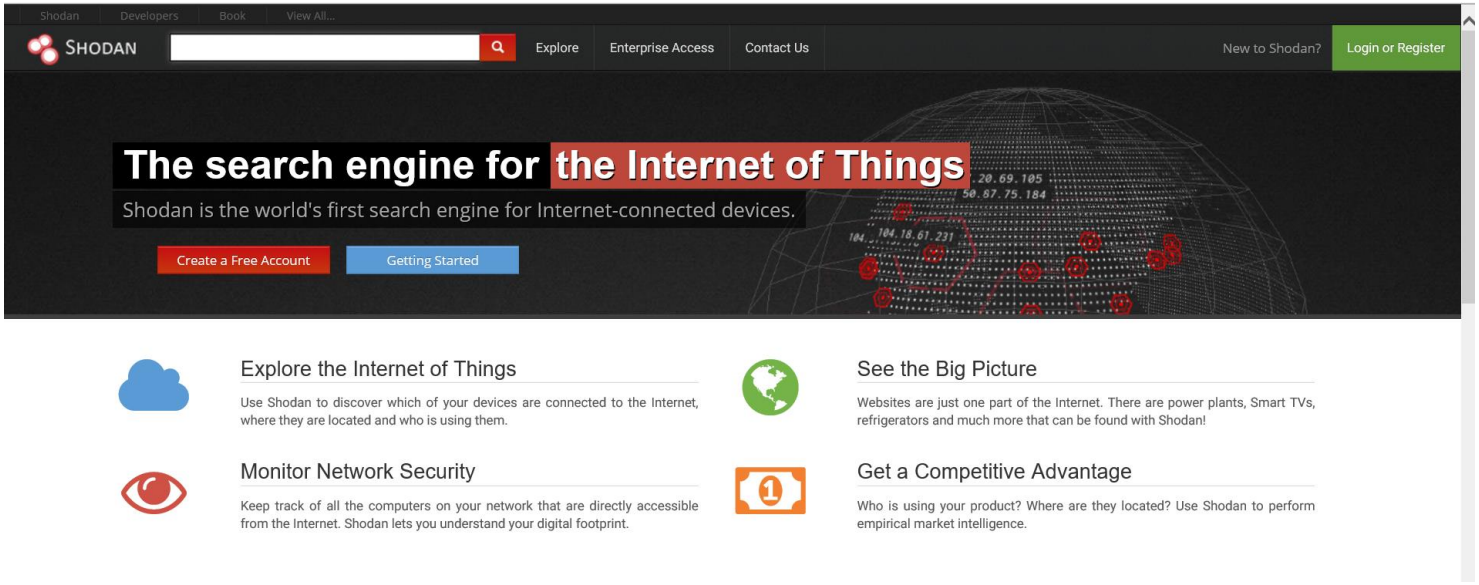
- **Huge growth with 20.4B devices online in 2017, 23.1B in 2018**



Risks with respect to the Internet of Things (IoT)

- **32% of IoT devices connect directly to Internet, bypassing traditional IT security controls**

- **If you want to get an idea of how insecure IoT is, go browse https://shodan.io**



Examples of vulnerabilities

- **An example of a risk was disclosed this week: “Strava Fitness App Shares Secret Army Base Locations”**
  - Strava's map includes the Helmand province of Afghanistan and shows the layout of operating bases via exercise routes
  - The base does not show up on the satellite views in both Google Maps and Apple Maps
- **Samsung’s smart TVs recording the sounds of the room they are in**
- **Multiple baby monitors have been hacked**

Why are IoT devices at risk?

- **IoT devices have a small version of popular operating systems on them (Linux, Android, Apple iOS, Windows IoT)**
- **Very hard to install regular patches/updates**
- **Vendors stop releasing patches to focus on their next big “thing”**
- **Current estimates are that 1M devices a month are being compromised**

Risks with respect to the Internet of Things (IoT)

What can you do?

- **Know what is connected to your network and what it does – Asset Management!**

- **Know what is running on the devices and who they talk to**

- **Treat IoT devices the same as you treat your desktops and systems (patching, hardening, monitoring, etc.)**

Risks with respect to the Internet of Things (IoT)

What can you do?

- **For adding new devices, perform an evaluation of the device and any risks**
  - How will the device be used from a business perspective?
  - What threats are anticipated and how will they be mitigated?
  - Who is responsible for monitoring for new attacks or vulnerabilities pertaining to the device?
  - What personal information is collected, stored or processed by the IoT devices and systems?

Current Cyber RISKs and ATTACKS

Current Cyber risks and attacks

- **Financially Sophisticated Cyber Criminals**
  - $1.5 Trillion in 2018 - $6 Trillion by 2021
  - If cybercrime was a country it would have the 13th highest GDP at $1.5 Trillion – And 4th by 2021
- **Denial of Service attacks have increased in frequency, potency and sophistication.**
  - In 2016 it cost $15 to $50/hr to have hackers take a site off-line for an hour
- **Self-learning Artificial Intelligence**
  - Malware that silently learns its environment, disguising itself and carefully choosing its actions
  - Automated “Sleeper” RansomWare

Current Cyber risks and attacks

- **Increase in IoT and IIoT attacks**
  - How much would you pay to *unlock* your data, thermostat, Smart TV, mobile phone, pacemaker, power gird?
- **Nation States Targeting Private Sector**
  - Corporate espionage of private sector for competitive advantage
  - ‘Hacked’ Out-of-the-Box hardware and software
- **Human Error from Increasing Complexity**
  - Opening malicious links or email attachments
  - Incomplete backups
  - Operational failures in Cyber Incident Response
  - Accidental data exposures

What is the message to remember?

Build your Defensible Position

- Identify your assets, risks and threats
- Identify how you compare to good security practice, based on your assets, risks and threats
- Put a plan in place to formally mitigate or accept the risks

What is the message to remember?

A good Defensible Position will help you say:

- We followed leading security practice (NIST, ISF, ISO27001/2)
- We regularly reviewed our risks, keeping up to date with the latest threats and vulnerabilities
- We had strong technical controls
- We had good security awareness
- We conducted Cyber breach simulation exercises
- We used independent experts to help improve our security
- We dealt with the incident in a timely and forensically sound manner
- We mapped these against prevention, detection and reaction to security incidents

How can KPMG help?

- **Companies talk about being a leader in information security, in Forester Research's ranking of Information Security Consulting Services Companies: KPMG was a leader in 2016 report and IS the leader in 2017 report.**
- **KPMG has a dedicated Cyber team of 40+ practitioners who can challenge management's thinking and approach. Our experts bring leading-edge thinking in Cyber Security consulting and can use that knowledge to help our clients' internal teams. We can benchmark your current Cyber Security posture against good practice to give you a view of how you compare to your competitors and the wider market.**
- **KPMG's Cyber Team offers a range of services to help your organization be in a Defensible Position to prevent detect and respond to cyber threats. We believe that cyber security should be about what you can do – not what you can't.**
- **Our full lifecycle of services cover all aspects of cyber security from the boardroom through to the back office, including cyber security strategy to breach response.**

Questions?

Thank you!

Be in a defensible position

Be cyber resilient