WorkED

CYBERSECURITY VIRTUAL EXTERNSHIP

PRIVATE SECTOR CYBERSECURITY

WorkED

WHAT IS THE PRIVATE SECTOR?

Focuses on **cyber threats** to small businesses, communications companies, mobile technology, cloud computing, and smartphone applications.

Run by individuals and companies **for profit** and is **not state controlled**. ... Companies and corporations that are government run are part of what is known as the public sector, while charities and other nonprofit organizations are part of the voluntary sector.

WorkED

WHAT ARE WAYS A COMPANY CAN BE BREACHED?

TECHNOLOGY

- Ransomware/Spyware/Malware/Phishing
- DDOS
- Weak Passwords
- Old Passwords
- Unsegmented Network

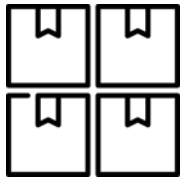
HUMAN ELEMENT

- Dumpster Diving
- Minimal Security
- Insider Threat
- Theft
- Accidental Disclosure

WorkED

DIFFICULTY IN PRIVATE SECTOR

With **so many different** companies and people **involved** in the private sector, there are lots of moving parts, making it **difficult to keep security**.



Suppliers and Vendors

Customers

Third Party companies

If one is compromised, then all could be

Skills Gap - 3 million unfilled jobs

WorkED

TARGETS?

Tight budgets and a historical “best left alone” approach to new technology mean the sector’s **falling behind the technology curve**, while user demand and flexible working create a need for bigger, looser networks with more mobile and virtual devices included.

Public sector organizations face a unique combination of cybersecurity threats. Being state bodies, they’re **attractive targets for hacktivists and state-sponsored hackers from abroad**; holding sensitive data makes them lucrative targets for conventional cybercrime.

Preparing to meet these threats isn’t just a matter of spending money and upgrading machines, though. It demands a cultural shift toward taking cybersecurity seriously. To close the loopholes which human error leaves in cyber defence, private and public sector organizations need to sponsor and recruiting the right talent.

WorkED

WHY MIGHT A COMPANY NOT SECURE THEIR DATA?

Expensive - Budget constraints are a constant issue across the public sector. IT managers are often told to move with the times and bring in the latest technology on a budget which is at best frozen and at worst being cut

Time Consuming - takes too long to train or become well versed in technology let alone security

Don't think it will be a factor - think company is too small and it won't be an issue. "That will never happen"

Too advanced / Old Fashioned - stuck in their ways, don't want to learn new complicated things

WorkED

PREVENTATIVES

Segmented Network

Updated Software

2 Factor **Authentication**

Hardened **Firewall**

Limited Access

Complex Passwords

WorkED

HOW IMPORTANT IS IT?

- A **medical record is worth ten times as much as a credit card number on the black market**. That's why 34.5% of data breaches around the world take place in healthcare, compared to 4.8% in banking. (Education and the military hover between the two, at 9% and 6.6% respectively.)
- Cyber attacks on private/public sector bodies also come from hacktivists -- people u**sing cyber attacks to protest, promote or demonstrate a political point**, like the hackers who shut down UK police websites and distributed stolen police data to oppose the arrest of Julian Assange in April 2019.
- The private sector is **vulnerable** not only because it's a politically and financially rewarding target, but also because the data it holds is so sensitive. Private sector organizations handle records of care, vulnerability and abuse; they hold intellectual property related to cutting-edge research; they represent a state body and its operations, and a successful attack on them is a successful attack on the state.

WorkED

WHAT ARE THESE METHODS?

DISTRIBUTED DENIAL OF SERVICE (DDOS)

When an overflow of information is sent to a system causing it to shut down.

This tells the intruder that the security is off and they have easier access while trying to penetrate the network.

It is like shutting off the electricity.

UNSEGMENTED NETWORK

When a company stores all of their information in the same place instead of storing it in multiple places. This way all of the information will not be available on one breach alone.

WorkED

LAYERED SECURITY/LAYERED DEFENSE

THE METHOD OF SECURING YOUR NETWORK WITH MULTIPLE TYPES OF SECURITY.

This way if a person is trying to gain access, they **have to use multiple methods of resources** to gain access to the information. The hope is that they are unable to beat all security methods or that the intruder takes so long to break the security, they can be caught.

WorkED

OVERVIEW OF 5 TYPES OF STRATEGIC RISK

COMPETITIVE RISK

Competitive forces that prevent achieving goals

FINANCIAL RISK

Financial loss, theft, misuse of funds, fraud

OPERATIONAL RISK

Safety, continuity of service, quality of service

REPUTATIONAL RISK

Public and employee perception

GOVERNANCE

- Legal and financial penalties for failure to meet requirements
- New requirements that impact business operation

WorkED

EQUIFAX BREACH

U.S. POPULATION 325.7 million

DATA ELEMENT STOLEN	IMPACTED U.S. CONSUMERS
NAME	147 MILLION
DATE OF BIRTH	147 MILLION
SOCIAL SECURITY NUMBER	146 MILLION
ADDRESS	99 MILLION
GENDER	27 MILLION
PHONE NUMBER	20 MILLION
DRIVER'S LICENSE NUMBER	18 MILLION
EMAIL ADDRESS	2 MILLION
CREDIT CARD NUMBER	209,000
TAX ID	97,500
DRIVER'S LICENSE STATE	27,000

SOURCE: Securities and Exchange Commission filing from Equifax

Between May 12th and July 29th of 2017, the **personal information of 147 million Americans was compromised** by the private credit reporting agency Equifax.

CAUSE

- Failure to update software
- Insufficiently segmented network design
- Inadequate encryption of customer information
- Ineffective breach technology

RESPONSE

- Locked down the breach on July 30, 2017
- Delayed disclosing until September 7, 2017

CONSEQUENCES

- $300 million settlement to consumers
- $170 million settlement to state and local governments
- $100 million in fines

LASTING IMPLICATIONS

- Identify theft: new accounts, terrorist entry, tax and benefit fraud
- Impersonation: access existing accounts, steal from consumers, steal government and corporate information

WorkED

EVOLVING TECHNOLOGY

- A brand new Iphone gets released every year along with new software.
- Microsoft releases updates to their software every 6 months.
- Major computer companies release a computer 3 times a year.

SOFTWARE NEEDS TO BE UPDATED IMMEDIATELY INCLUDING ANY PATCHES.

CONTINUING EDUCATION NEEDS TO BE DONE YEARLY TO KEEP UP.

WorkED

FACEBOOK / INSTAGRAM

Between early 2012 and January 2019, 2,000 **Facebook employees viewed passwords** of Facebook and Instagram users 9 million times.

CAUSE

- Storage of passwords in readable plaintext
- Permissive access to 20,000 Facebook employees

RESPONSE

- Delayed disclosing until late March 2019, after an employee notified media
- Disclosed in an old blog post and only to “affected users” by prompting a password change

USER IMPLICATIONS

- Privacy violations: private messages, photographs, videos, and personal information
- Password reuse: 65% of people use the same password for multiple or all accounts
- Stalking/harassment
- Impersonation

CONSEQUENCES

- Twenty years of FTC oversight of privacy practices for all products of Facebook, WhatsApp and Instagram
- $5 billion settlement with FTC

WorkED

DDOS ATTACK AGAINST DYN

In October 2016, DYN was hit with a DDoS attack which interrupted the **service of 80 websites**, including Amazon, Netflix, Airbnb, Spotify, Twitter, PayPal and Reddit.

CAUSE

- 100,000 malware-infected devices, including radios, smart TVs and printers, that bombarded Dyn with Internet traffic requests

OUTCOMES

- Users unable to access affected websites for one day
- Estimated $110 million in losses
- 14,500 customers dropped Dyn

WorkED

COMMON TOOLS

NMAP - A.KA. NETWORK MAPPER

- Free scanner to see who or what is on your network
- IDS/IPS - Intrusion Detection System/Intrusion Prevention System
- IDS alerts network for security violations and possible malicious activity
- IPS - monitors incoming packets or traffic for harmful threats

PENETRATION TESTING

- Legally trying to hack your a network to find vulnerabilities

ANTIVIRUS SOFTWARE

- Software to help prevent against spoofing, malway, spyware, etc

FIREWALLS

- Barriers within network to block unwanted access

WorkED

CYBERSECURITY VIRTUAL EXTERNSHIP

PRIVATE SECTOR CYBERSECURITY

QUESTIONS?

THANK YOU

CREDENTIAL THEFT

ESC 20 Serving the Educational Community

workED