Cybersecurity & Telecommunicating

Stop attacks before they start.

Pete Jarvis
Vice President, Business, Polyverse
pete@polyverse.com
Our Problem: Constant Attack

Today, your valuable data is unprotected for an average of 102 days

- This excludes the time before the vulnerability is discovered
  - Attacks on average are in use for 9 months before discovery

*State of Endpoint Security, 2018, Ponemon Institute*
Result: Cyber Threat Escalation

Complexity of Cyber Attack Capabilities are Growing

BUSINESS IMPACT:
- Citizen trust
- Cost to protect
- Legal/ regulatory
- Critical infrastructure

EVOLUTION OF TECHNOLOGY

DATA EVERYWHERE; USER EXPERIENCE DRIVEN
- Wearable technology
- Internet of things
- Smart devices
- Drones
- Artificial intelligence
- Mobile payment
- Etc.

DATA IN SECURE BUSINESS SYSTEMS
- Mainframe systems
- Internetworking
- Emergence of open systems

INTERNET ACCESS AND HIGHLY CONNECTED SYSTEMS
- Online access to citizen data
- Advances in internetworking
- Citizen self service

ACCESS ANYWHERE & ANYTIME
- Integrated online eligibility systems
- Big data
- Cloud
- Mobile

1990s

2000s

2010-2014

NOW
DIGITAL WORKPLACE: COMPONENTS

Overview

- Business applications
- Internal communication
- Intelligent search engines
- Automated processes
- Cloud/external applications
- Self-service portals
- Global communication
- Cloud/web services
- Internal services
The digital workplace allows knowledge to be shared regardless of location, time and device. It combines company software systems onto a single platform and provides each employee with their own dashboard of functions and information.
Cyber Security is Complex yet Simple

Initial Access
Execution
Persistence
Privilege Execution
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
THREATS

Phishing

ATTACKER

Aims to easily obtain sensitive and personal data

TROJANS & WORMS

Creates fake messages that include links to online shops, social networks, payment services, etc.

VICTIM

Victims enter personal and confidential information unsuspectingly
Various new forms of malware appear on the internet every day.

Nest undetected in computer systems or creep in during downloads.

TROJANS & WORMS

ARE SENT VIA INFECTED EMAILS

Can transfer sensitive data such as passwords, banking information, personal data.
THREATS

Botnets

ATTACKER

Networks consisting of several computers

BOTNETS CONTROLERS

INFECTED

Can send infected and dangerous (spam) emails

Can steal personal information (e.g., Passwords)

TARGET

Can attack all IT systems
Cybersecurity Checklist

- What is our plan to respond to a data breach?
- How do we monitor our systems and prevent breaches?
- How often do we verify the effectiveness of our security?
- Is our security clear and consistent?
- Are third parties really securing our most valuable information?
- Are we adequately insured?
- Do our security goals align with business priorities?
- How much is the issue of security integrated into your business?
- Do we have the basic rights for security measures?
- Have we identified and protected our most valuable processes and information?
- Do we treat cybersecurity as a business or an IT responsibility?
# Cybersecurity Questions for a Business

<table>
<thead>
<tr>
<th>Question</th>
<th>✓/☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do we treat cybersecurity as a business or IT responsibility?</td>
<td>☐</td>
</tr>
<tr>
<td>Do our security goals align with business priorities?</td>
<td>☐</td>
</tr>
<tr>
<td>Have we identified and protected our most valuable processes and information?</td>
<td>☐</td>
</tr>
<tr>
<td>Does our business culture support a secure cyber environment?</td>
<td>☑</td>
</tr>
<tr>
<td>Do we focus on security compliance or security capability?</td>
<td>☐</td>
</tr>
<tr>
<td>Are we certain our third-party partners are securing our most valuable information?</td>
<td>☐</td>
</tr>
<tr>
<td>Do we regularly evaluate the effectiveness of our security?</td>
<td>☐</td>
</tr>
<tr>
<td>Do we have a plan for responding to a security breach?</td>
<td>☐</td>
</tr>
<tr>
<td>CHECKLIST</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td><strong>HELPFUL TIPS</strong></td>
<td></td>
</tr>
<tr>
<td>Are the Internet services that are being accessed and used safe?</td>
<td></td>
</tr>
</tbody>
</table>
| Are employees trained for cyber attacks? ✔ |}
| Are mobile devices such as laptops, smartphones and tablets protected from a data breach? |
| Is a cyber attack from outside the corporate network possible? What are your external access options? |
| Are there any contingency strategies and exercises? ✔ |
| Are there periodic updates for operating systems and programs |
| Do you know the email sender who is requesting data? |
| Do I trust the source of the links/ download? |
Resources:
https://www.uschamber.com/CybersecurityEssentials
DIGITALIZING WORKPLACES
The digital workplace: the foundation for remote work

YESTERDAY
OFFICE WORKSTATION
- Desktop computer / PC
- Landline telephone
- Internet connection / LAN
- Printer

TODAY
DIGITAL WORKSTATION / HOME OFFICE
- Laptop
- Tablet
- Smartphone
- Cloud Storage Software services
- WiFi
- Video conferencing software

14/7/20
Cybersecurity & Telecommunicating
CURRENT ISSUES
Legal aspects concerning remote work

LEGAL ENTITLEMENT

Form a legal standpoint, employees do not have an inherent right to work from home.

Without specific arrangements or contractual regulations, employees remain obliged to appear at the workplace.

NO OBLIGATION TO WORK REMOTELY

At the same time, employees cannot be forced to work from home.

The employer’s right to issue directives does not constitute sufficient basis for mandating remote work.

EMPLOYERS’ DUTY OF CARE

The employer has a duty of care towards their employees and must consider any threat associated with their presence in the workplace.

If an employee is in home quarantine, they are obliged to work remotely unless they are written up sick.
REMOTE WORK: IMPLEMENTATION
Steps towards working from home

PROVIDE TOOLS AND ACCESS

- Provide hardware
- Appoint a software administrator/officer
- Messaging platforms
- Video and team-call software
- Cloud documentation software
- Cloud storage for data exchange

PREPARE AND BRIEF YOUR TEAM

- Acquaint your employees with the tools
- Select a channel/platform
- Define rules for communication
- Which communication tool should be used in which situation?

INTERACT WITH YOUR TEAM

- Arrange availability
- Set up accounts on online messaging platforms
- Agree on roles and responsibilities
- Visualize the processes
- Maintain communication and interaction online

MAKE ADJUSTMENTS

As soon as the main processes for working from home have been set up:

- Aim to optimize the processes
- Experiment with the tools
- Continuously review and improve the process and how people interact, especially when working from home
REMOTE WORK: GUIDELINES
Recommendations for good communication and organization

**SOCIAL INTRANET**
- Exchange information over your own social intranet.
  - Pass on information from management
  - Promote teamwork
  - Build team spirit
  - Encourage social communication

**UPDATES FROM MANAGEMENT**
- Provide daily updates from management via email or digital channels.
  - Keep employees aware of current strategies
  - Share information
  - Motivate and be available to employees
  - Communicate any adjustments required for remote work

**SENIOR MANAGEMENT MEETING**
- Carry out management-level video conferences several times a week.
  - Share your problems and solutions
  - Learn from each other
  - Reinforce team spirit

**DATA ACCESS AND DATA EXCHANGE**
- **VPN access:**
  - Remote access to the company’s internal network
- **Issues with data exchange via cloud services:**
  - Security and privacy
  - Access rights
  - Backup
## REMOTE WORK: LEADERSHIP

**Trust is far better than absolute control**

<table>
<thead>
<tr>
<th>LEADERSHIP STYLE/COMMUNICATION</th>
<th>PROCESSES AND PROCEDURES</th>
<th>REMOTE CORPORATE CULTURE</th>
<th>GOALS AND OUTCOMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Communicate information</td>
<td>– Agree on guidelines and directives</td>
<td>– Culture Map: intercultural teams</td>
<td>– Focus on results instead of hours worked</td>
</tr>
<tr>
<td>– Offer support/feedback and constant contact</td>
<td>– Set rules for team communication and work hours</td>
<td>– Accept flexible working hours and working methods</td>
<td>– Clear targets</td>
</tr>
<tr>
<td>– Digital mindset: trust in employees’ motivation</td>
<td>– Maintain your regular meeting schedule</td>
<td>– Create cohesion despite social distancing</td>
<td>– Trust instead of control</td>
</tr>
<tr>
<td>– Don’t fear loss of control</td>
<td>– Daily check-ins are a must</td>
<td>– Encourage self-development/ongoing training for employees</td>
<td></td>
</tr>
<tr>
<td>– Hand over responsibility</td>
<td>– Daily standups via video call (15-30 minutes) are a great idea</td>
<td>– Provide online learning/coaching and digital learning groups</td>
<td></td>
</tr>
<tr>
<td>– Lead through clear goals; trust, empathy and motivation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REMOTE WORK: TOOLS
The scope of the tools supporting your company when working remotely

COMMUNICATION
Tools enabling communication are essential to working from home. Use chats, video conferences or your phone for this.

ORGANIZATION / DOCUMENTATION
There are many programs offering cloud services. Use them to synchronize calendars and share tasks and notes.

DATA EXCHANGE / DAILY BUSINESS
Project management tools allow employees to organize and exchange data from home.

SUPPORT TOOLS
Little tricks and hacks to help you optimize your work. Screenshots can be used to simplify written communication, for example.
## DEFINITION

### Glossary

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT (ADVANCED PERSISTENT THREAT)</td>
<td>Hackers who provide time and resources (money) in large quantities with long-term goals</td>
</tr>
<tr>
<td>SPOOFING</td>
<td>Attempting to conceal another’s identity in networks</td>
</tr>
<tr>
<td>KILL SWITCH</td>
<td>Hidden software that can be activated by an outside source in emergency situations</td>
</tr>
<tr>
<td>JAMMING</td>
<td>Intentional disruption of radio communication</td>
</tr>
<tr>
<td>DEFACEMENT</td>
<td>Hacking a website’s content, electronic graffiti</td>
</tr>
<tr>
<td>BACKDOOR</td>
<td>A hidden part of software to access a computer</td>
</tr>
<tr>
<td>BOTNET</td>
<td>A network of computers that can be remotely controlled by botmasters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TERM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXPLOIT</td>
<td>Vulnerabilities in software that can specifically be exploited by programs or codes</td>
</tr>
<tr>
<td>ZERO DAY</td>
<td>A hole in the software that is unknown to the manufacturer</td>
</tr>
<tr>
<td>PHISHING/ SPEAR PHISHING</td>
<td>Through tricks, consumers are misled into revealing personal or sensitive information / a targeted and personalized phishing attack by email</td>
</tr>
<tr>
<td>OSNIT (OPEN SOURCE INTELLIGENCE)</td>
<td>Information collected from public sources</td>
</tr>
<tr>
<td>MONEY MULE</td>
<td>People who are hired by criminals to accept and forward money from customers, but are deceived into thinking they are working for a legal organization</td>
</tr>
<tr>
<td>MALWARE</td>
<td>The generic term for malicious programs and viruses for performing unwanted and harmful functions</td>
</tr>
<tr>
<td>DOS/DDOS (DENIAL OF SERVICE)</td>
<td>The unavailability of a previously accessible service (DoS)/ if a larger number of different systems are overloaded, it is known as distributed denial of service (DDoS).</td>
</tr>
</tbody>
</table>
Reading Recommendations

References

Cybersecurity Is Everybody's Business: Solve the Security Puzzle for Your Small Business and Home

- https://www.amazon.com/dp/B07X4419B6/ref=rdr_kindle_ext_tmb

Spear Fishing - Arun Vishwaneth. Black Hat talk is worth reviewing, Arun is doing interesting work on identifying and determining the risk profile of different people within an organization.


Social Engineering: The Science of Human Hacking

- https://www.amazon.com/dp/B07F24YV2M/ref=rdr_kindle_ext_tmb

The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities

- https://www.amazon.com/dp/B004XVIWU2/ref=rdr_kindle_ext_tmb

Computer Security by Matt Bishop

- https://www.amazon.com/dp/B07KXYK9XH/ref=rdr_kindle_ext_tmb