CYBER SECURITY
AND MITIGATING RISKS
WHO

Tom Stewart
Associate Director
Technology Consulting
Chicago Technical Security Leader
Protiviti
PRESENTATION AGENDA

START
HACKING DEFINITION
BRIEF HISTORY
TYPES
COMPUTER HACKING
MOTIVATIONS
RISKS
CONTROLS
4 SIMPLE STEPS
FINISH
“Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose.”

*Computer hacking* refers to the technique or process by which an individual attempts to gather information or gain access to a computer system. People who engage in computer hacking activities are often called *hackers*.

**There is more than one type of “hacking”**
MORE THAN ONE
Types of Hacking.
Once only a hobby for few, quickly turned into a vehicle for criminal enterprises and garnered the attention of mainstream culture.
A new wave of hackers has emerged based not on financial gain but rather social values.
**HACKER TYPES**

**WHITE HAT**
- Good Guys; Non-Malicious Intent; “Ethical Hacker”

**BLACK HAT**
- Bad Guys; Malicious Intent; “Cracker”

**GREY HAT**
- White and Black Hat; Notifies Administrator of Issue

**BLUE HAT**
- Outside Consulting Firm that Tests a System Prior or After Launch

**SCRIPT KIDDIES**
- Little Knowledge; Uses Pre-Packaged Tools

**HACKTIVIST**
- Uses Hacking to Announce a Social, Religious, or Political Message; “WikiLeaks”
MODERN HACKING
Types of Computer Hacking.

VULNERABILITY EXPLOITATION
Exploiting system flaws to obtain access to data or networks

SOCIAL ENGINEERING
Exploiting human emotion to gain access to personal information

WIRELESS
Exploiting wireless flaws to remotely obtain access to data or networks
3 STEPS TO VULNERABILITY EXPLOITATION

While exact techniques differ, modern vulnerability exploitation generally follows three set phases.
SOCIAL ENGINEERING

3 Types

PHYSICAL
Key Loggers
Virus Installs
Remote System Setup.

ELECTRONIC
Phishing Emails
Information Gathering

TELEPHONIC
Telephone Calls
Information Gathering
WIRELESS

01’ Major Threats
UnAUTHORIZED “ Rogue” ACCESS POINTS
New devices with wireless included

02’ Compromise Internal Networks
CONFIDENTIALITY
INTEGRITY
AVAILABILITY

03’ Use or Disrupt Resources
Wireless DoS
Inject traffic into internal networks
Drive-by spammers
HACKER MOTIVATIONS
What makes them go?

- Curiosity and Challenges
- Reputation and Notoriety
- Money and Personal Gain
- Hactivism and Social Rights
“It takes twenty years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.”
– Warren Buffett

RISK TYPES

- Resulting in reduced customer and vendor confidence
- Resulting in the loss of productivity and increased operational costs
- Resulting in fines or legal action
- Resulting in employee accountability issues
CONTROL FRAMEWORKS
How Do We Protect Ourselves?

NIST CSF
ISO 27002
Cobit
MULTI-FACTED APPROACH

- Automated Processes and Preventative Controls
- Manual Processes and Detective Controls
RISK CONTROL
Management

Do I know my risks regarding my information?

- Roles and Responsibilities
- Risk Assessment

Example Controls

Roles and responsibilities for data protection have been clearly defined and assigned to specific individuals.

Accessible data within the functional area is identified, classified, and inventoried in accordance with corporate Data Classification Standards. Classification of data is based on the importance of the asset, its business value and its associated security requirements.
Am I in compliance with all applicable privacy laws and regulations?

- Collection and Usage of Personal Data
- Notice, Consent, and Quality
- Knowledge Sharing

Example Controls

Personal Data should only be used in compliance with communicated privacy policies to customers, as well as applicable privacy laws and regulations.

All procedures have been designed to protect the privacy of Personal Data in compliance with current data privacy laws.

A written procedure is in place to confirm packaged knowledge from other sources can be utilized.
RISK CONTROL
Information Security

- Management
- Data Privacy
- Information Security
- Physical Security
- Incident Response
- Training and Awareness
- Vendor Management

Is my information protected?

- Access Rights
- Authentication
- Storage
- Transmission
- Backups
- Systems Security
- Network Security
- Information Disposal
- Application Development and Management

Example Controls

Access rights to confidential data are defined and documented.

Access to sensitive information is controlled by authentication methods that comply with current industry standards.

The technology and processes used to store sensitive data are in accordance with current industry standards.
### RISK CONTROL

Physical Security

<table>
<thead>
<tr>
<th>Management</th>
<th>Data Privacy</th>
<th>Information Security</th>
<th>Physical Security</th>
<th>Walkthroughs</th>
</tr>
</thead>
</table>

#### Is my information physically secure?

- Physical Security
- Walkthroughs

#### Example Controls

Physical security controls are in place to prevent unauthorized physical access.

Unscheduled physical walkthroughs are performed to check compliance with information security controls.
**RISK CONTROL**

**Incident Response**

- Management
- Data Privacy
- Information Security
- Physical Security
- **Incident Response**
- Training and Awareness
- Vendor Management

---

**Am I prepared in the event that a breach occurs?**

- Security Breach Response and Reporting
- Root Cause Analysis

---

**Example Controls**

A written procedure is in place for the prompt reporting of any known or suspected security breach.

Technology is in place to detect breaches.

A process is in place after a breach to determine root causes.
**Training and Awareness**

- Initial Training
- Ongoing Training and Awareness
- Roll-On and Roll-Off

**Example Controls**

Personnel are required to complete training outlining the proper handling and protection of sensitive information prior to being granted access to sensitive information.

Data protection training and awareness is communicated on an on-going basis and is updated annually.

Roll-On and Roll-Off procedure is in place to (a) help to ensure personnel rolling onto and off the project are made aware of the requirements with respect to information protection and (b) prevent sensitive information from other projects from entering the current project environment.
Do my vendors securely protect my information?

- Vendor Compliance

Example Controls

A process is in place to protect against privacy concerns with regards to vendors or other third parties that handle confidential information on behalf of the company.

VPN access is appropriately restricted to only those systems necessary to perform services.
4 SIMPLE STEPS
Where to go from here.

01 PERMISSIONS
File Shares, Applications, Vendors

02 PATCHING
Operating System, Application

03 SYSTEM HARDENING
Network Devices, Firewalls, Servers, Workstations

04 PROACTIVE TESTING
Simulated penetration testing and vulnerability assessments for low hanging fruit
Q & A

Tom Stewart
Associate Director
Technology Consulting
Chicago Technical Security Leader
Protiviti