Cyber Security for Small Companies

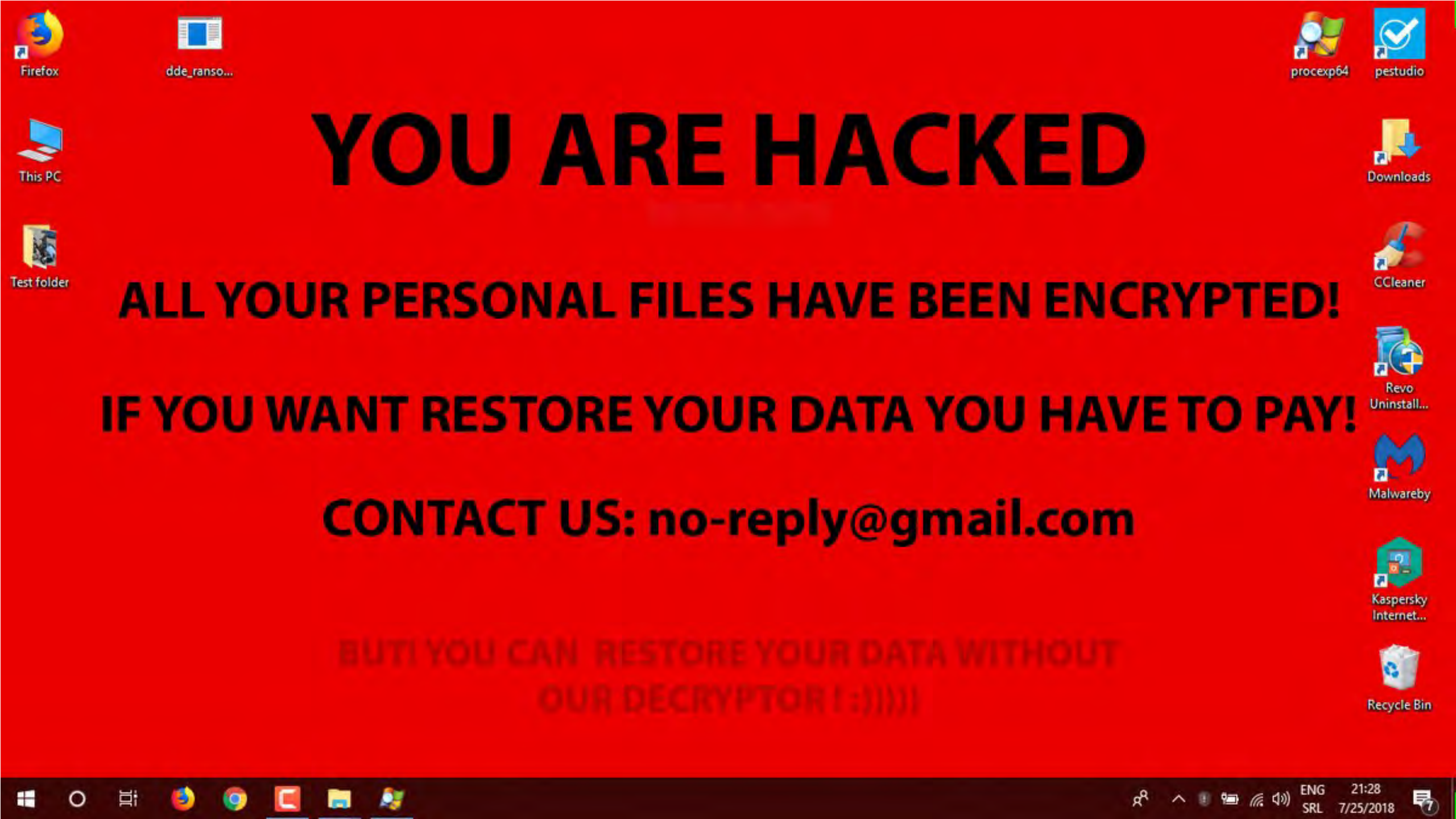
ASA 2019 Annual Conference

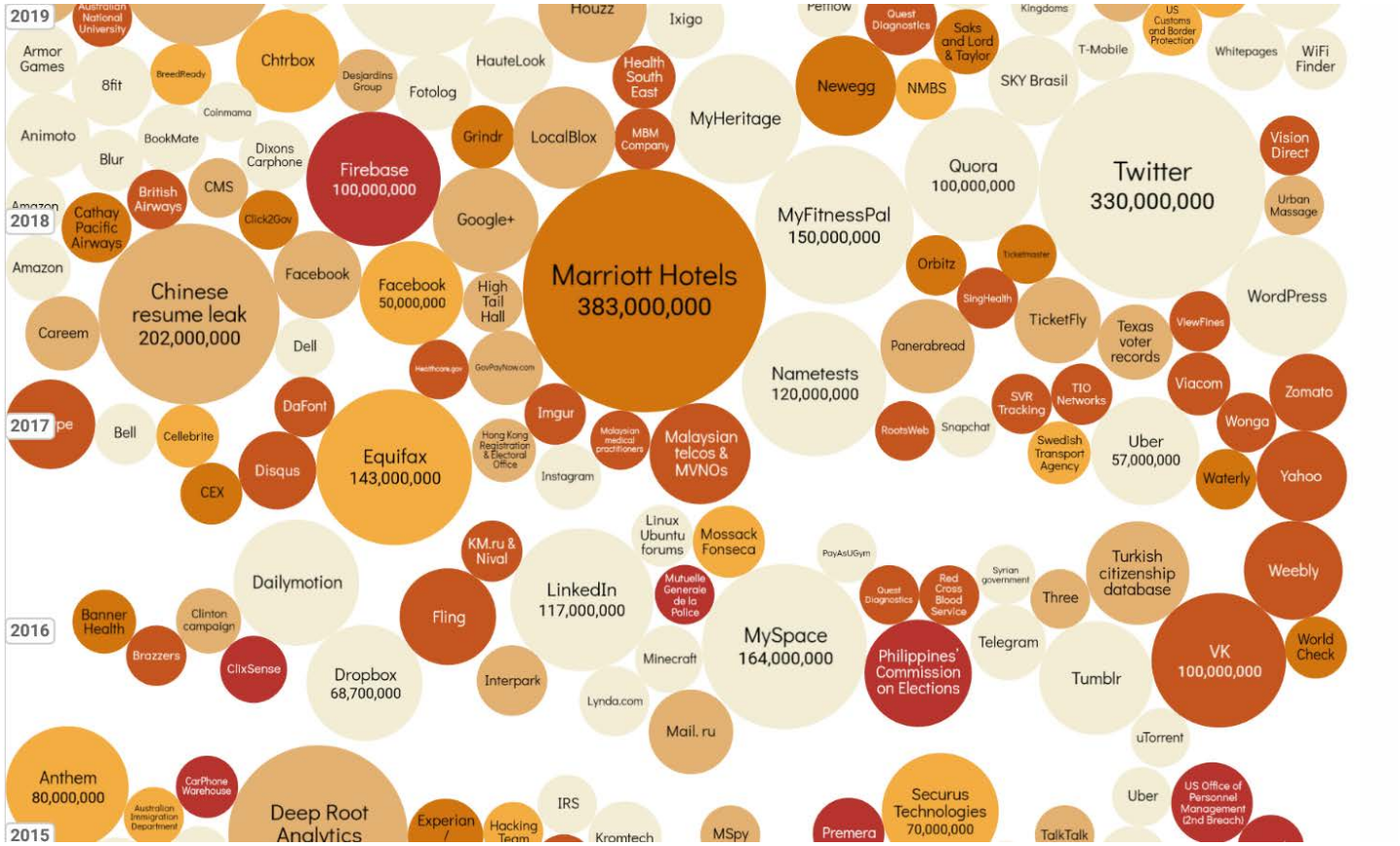
the core solution.com
ISO Experts for Small Business

Today's Presenter

Scott Dawson, President of Core Business Solutions

www.thecoresolution.com


Firefox
dde_ranso...
procexp64
pestudio
This PC
Downloads
Test folder
CCleaner
YOU ARE HACKED
ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!
IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!
CONTACT US: no-reply@gmail.com
Revo Uninstall...
Malwareby
Kaspersky Internet...
BUTI YOU CAN RESTORE YOUR DATA WITHOUT OUR DECRYPTOR ! :)))))
Recycle Bin
ENG
SRL
21:28
7/25/2018

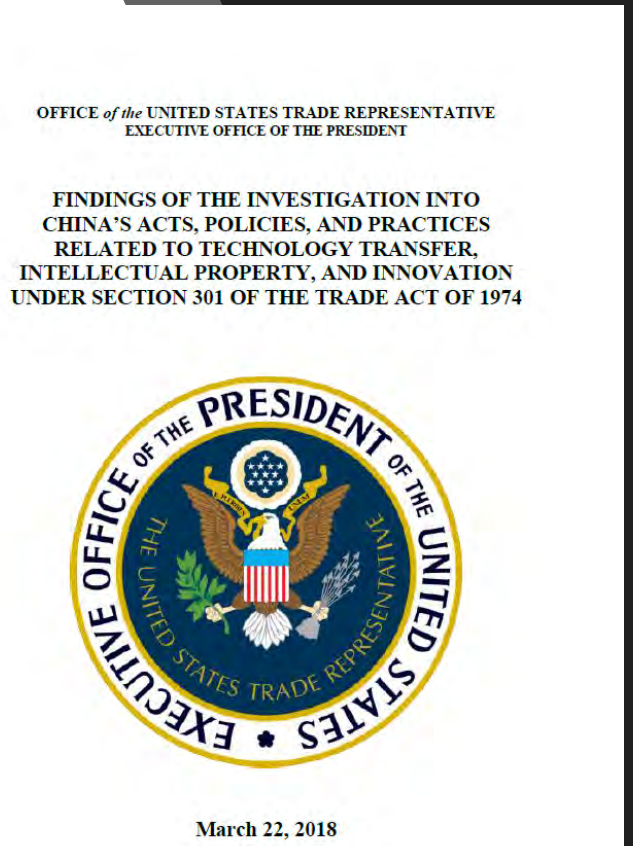


Who Gets Hacked?

Source:

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Extent of damage



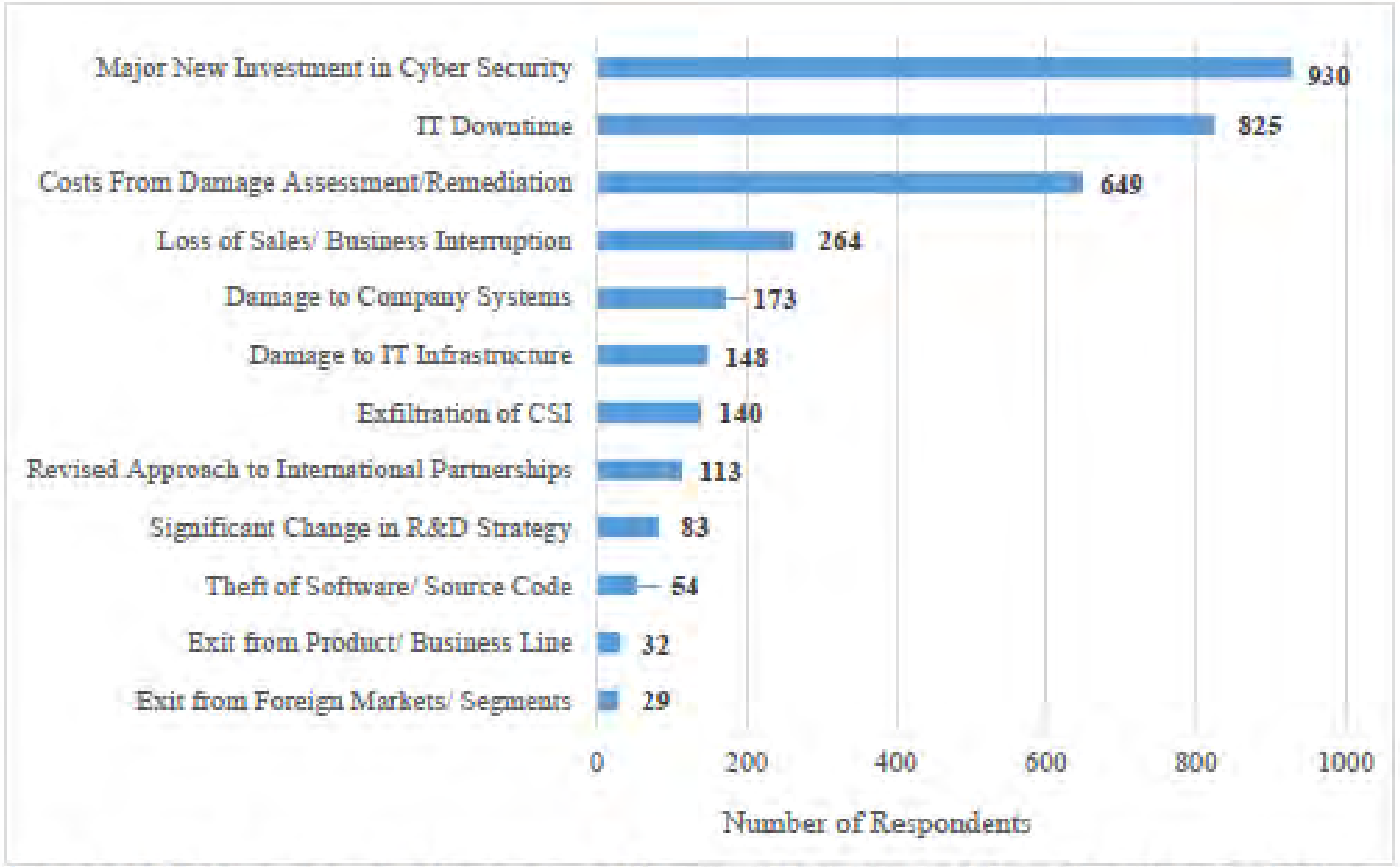
OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE
EXECUTIVE OFFICE OF THE PRESIDENT

FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974

March 22, 2018

- China's cyber intrusion and cyber theft activities harm U.S. business interests in a variety of ways. It can be difficult to assess the full burden on U.S. commerce because of chronic under reporting, companies being unaware that their network have been compromised or being unaware of the extent of the damage done. Nevertheless, a recent survey conducted by the Bureau of Industry and Security (BIS) contains the responses of more than 8,000 companies in the United States about the impact they face from malicious cyber activity from all sources. Respondents noted the following impacts in descending order:

Impact of Cyber Attacks



Source: U.S. Department of Commerce, Bureau of Industry and Security, Ongoing Defense Industrial Base Assessment.

Source: "Measuring and Managing the Cyber Risks to Business Operations," conducted by the Ponemon Institute, December 2018

What is Cyber Security?

- Steps we take in protecting sensitive data, computer systems, networks and software applications from cyber attacks.

The CIA Triad: Protecting Your Information

Internet-Enabled Crime

- Criminals see lower risks and high rewards from cyber crime than through “physical” crime.
- Illegal activities
  - Stealing information
  - Disrupting operations
  - Holding information “hostage”
  - Altering information
- Malicious activities
  - Infecting systems
  - Denying access

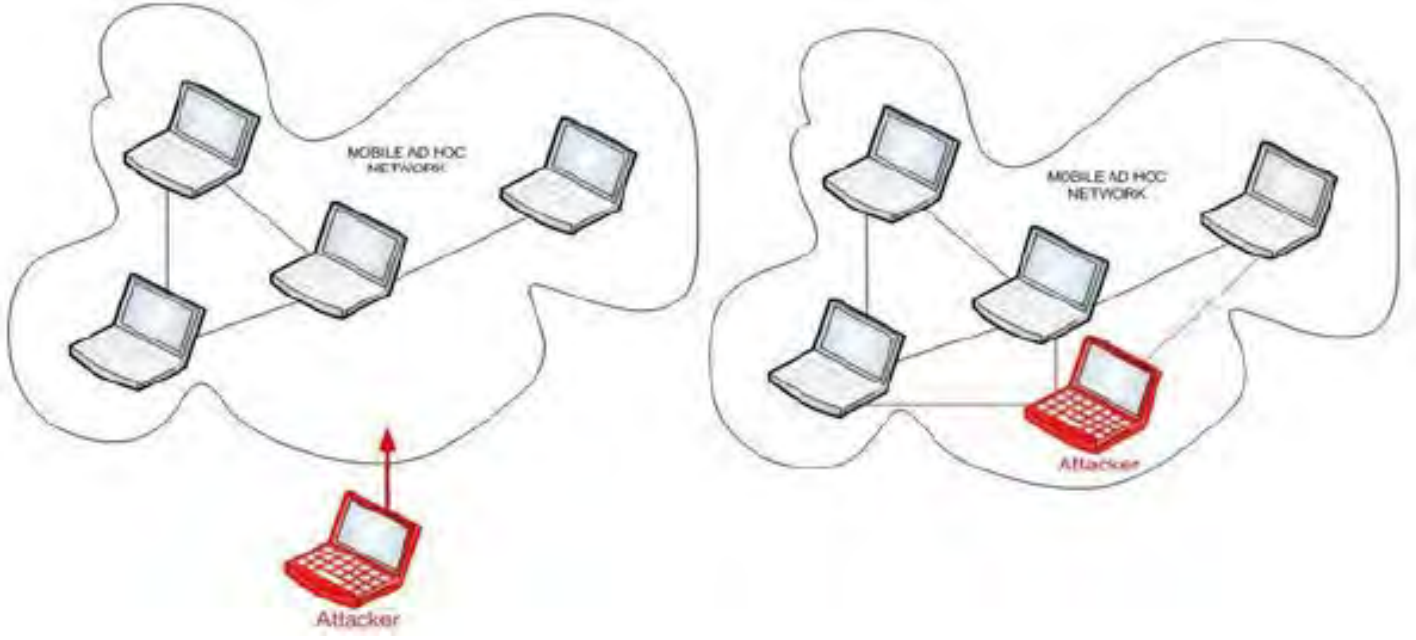
Where Does an Attack Come From?

External Attacks

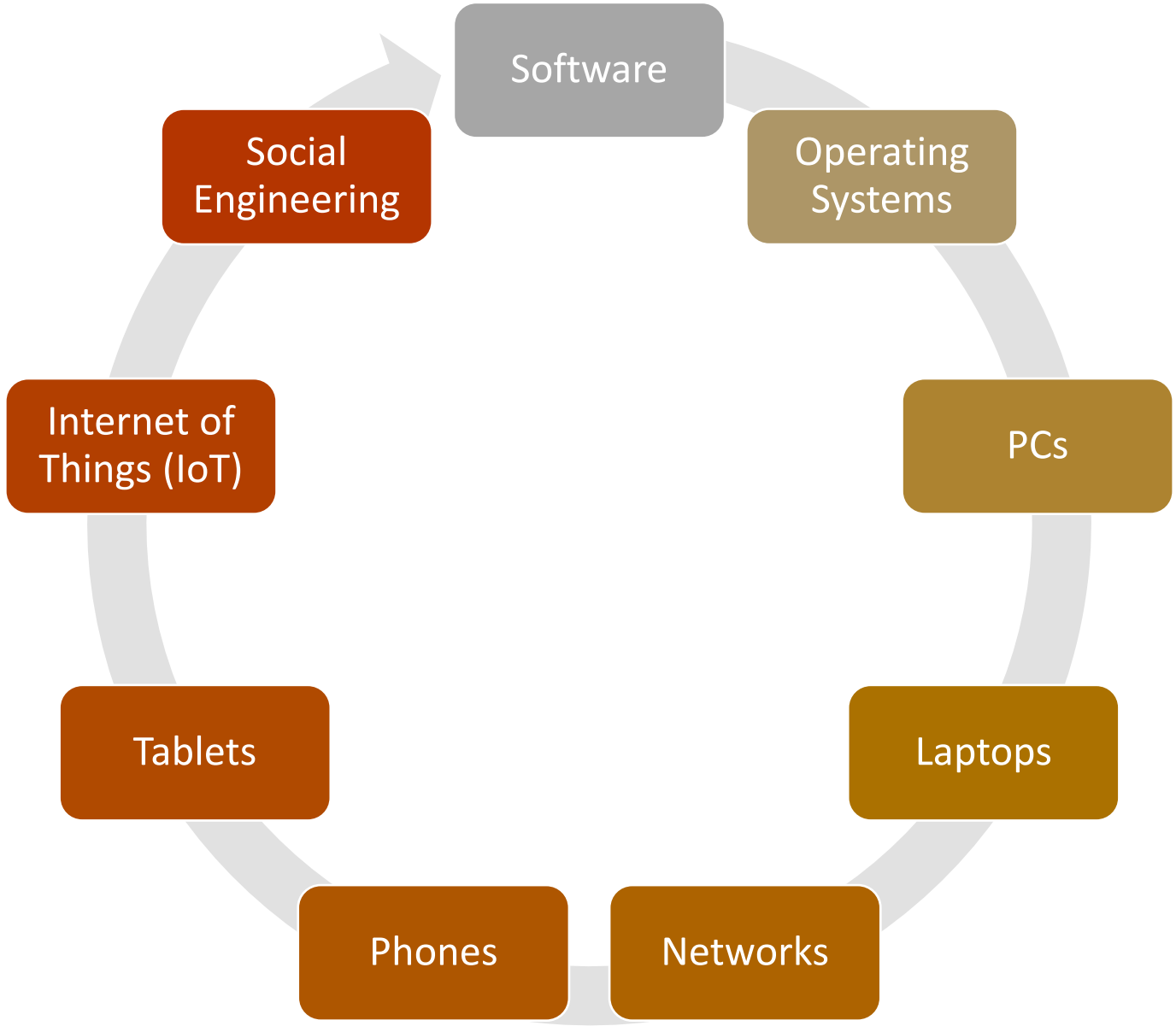
- Requires either valid credentials or exploitation of a vulnerability to access the system

Internal Attacks

- Can be hard to prevent because insider may have valid credentials to access the system



How Can Hackers Attack Us?

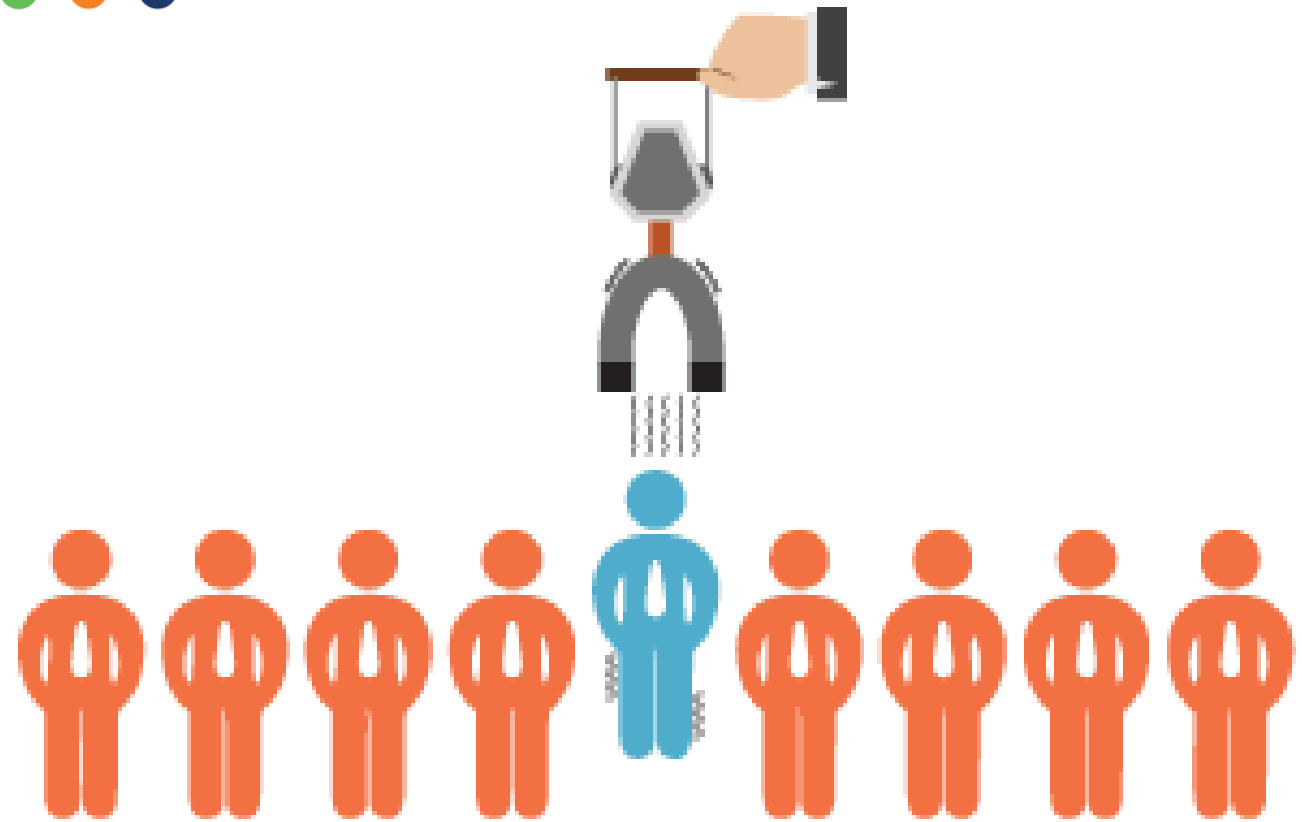


Cyber Threat Examples

Spam

Using electronic messaging systems to send unsolicited messages (spam), especially advertising, as well as sending messages repeatedly on the same site.

Security Hint: Never click on or respond to a Spam message.



Social Engineering

The Art of Human Hacking

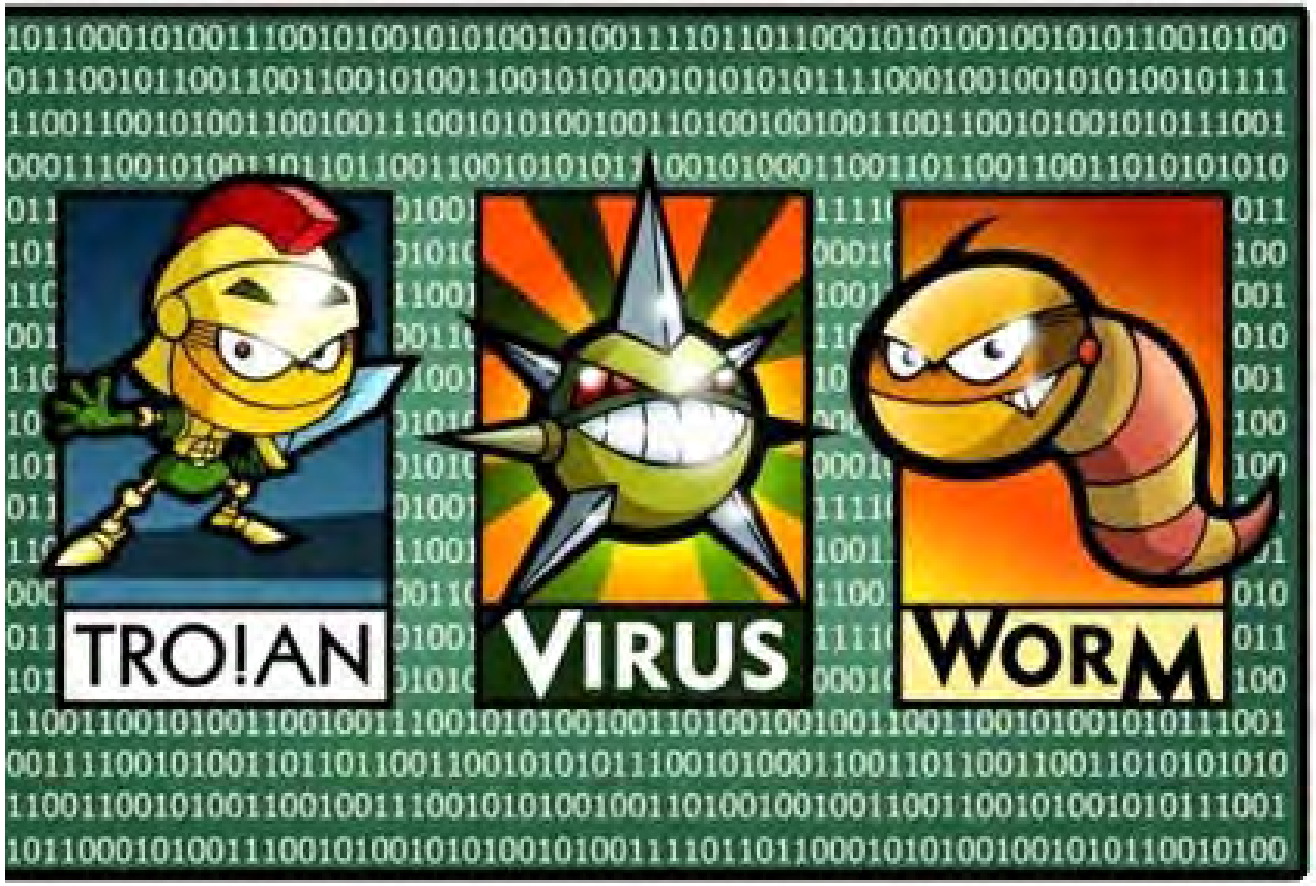
- A non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.
  - Phishing
  - Baiting
  - Pretexting
  - Quid Pro Quo

Phishing

- The attempt to acquire sensitive information such as usernames, passwords, and credit card details by pretending to be a trustworthy source.
- It is one of the most common Cyber Crimes.

Malware

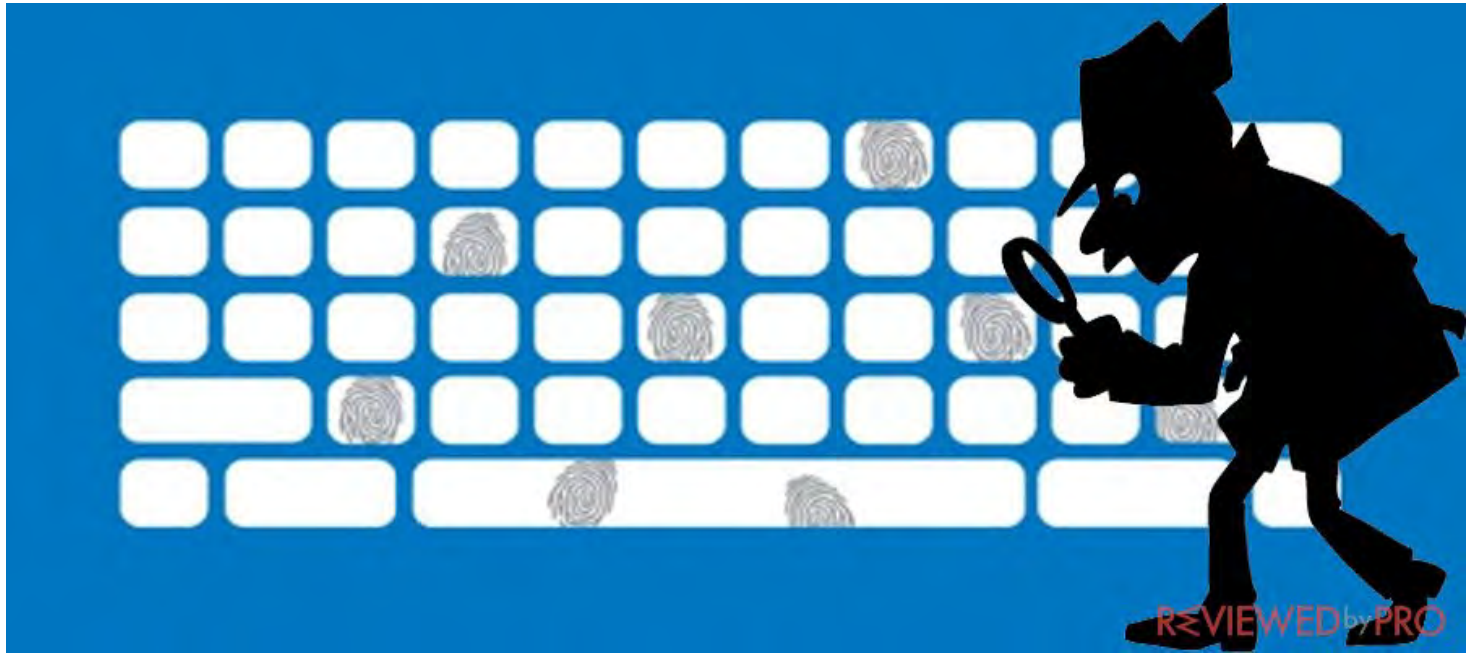
- **Trojan Horse** - A program that seems to be doing one thing but is actually doing another. It can be used to set up a back door in a computer system, enabling the intruder to gain access later
- **Virus** – malware attached to a carrier such as an email or electronic document
- **Worm** – malware that can autonomously replicate itself without a carrier, using information about connected computers



Ransomware

- A type of malware that encrypts a user's computer or company network and "demands" that the user pays a "ransom" to remove the encryption. If payment is not received, information is unusable or destroyed.

Key Loggers



A type of malware that captures key strokes and sends these to a remote system.

Used to try and get personal information to gain access.

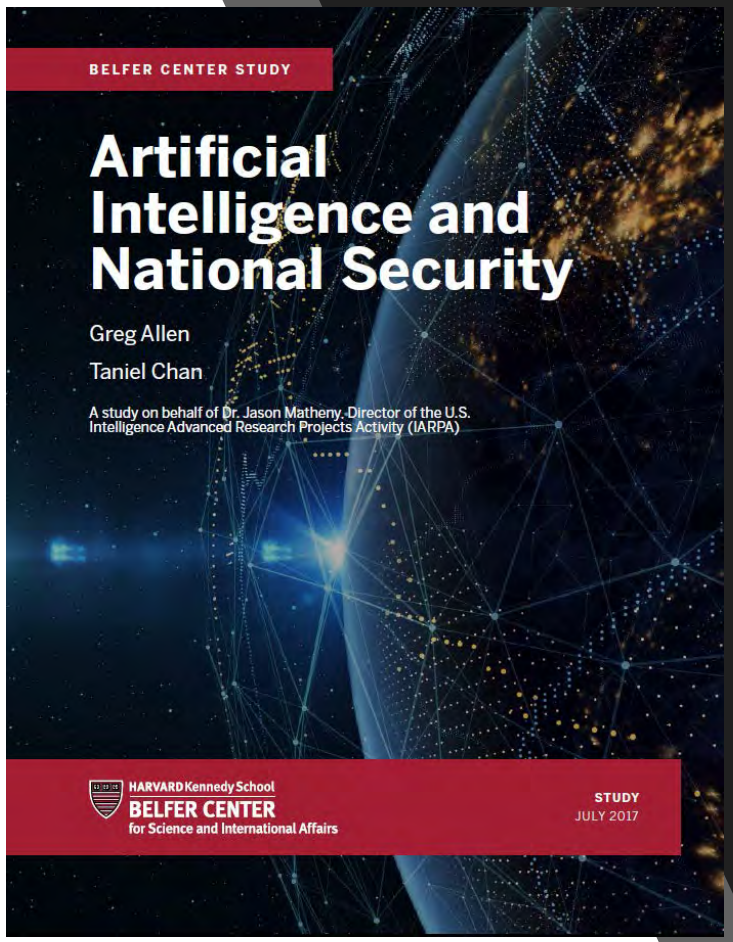
Trojan Horse

- A program that seems to be doing one thing but is actually doing another.
- It can be used to set up a back door in a computer system, enabling the intruder to gain access later.

Latest Cyber Threats

Industrial Control Systems (ICS) Security

- 2017 ICS THREAT REVIEW
  - 2017 was a watershed year in industrial control systems (ICS) security largely due to the discovery of new capabilities and a significant increase in ICS threat activity groups.
  - Cybersecurity risks to the safe and reliable operation of industrial control systems have never been greater.



AI Automated Attacks

- "With an APT, the attacker is actively hunting for weaknesses in the defender's security and patiently waiting for the defender to make a mistake."
- "Hunting for weaknesses" activity will be automated to a degree that is not currently possible and perhaps occur faster than human-controlled defenses could effectively operate.
- "Any actor with the financial resources to buy an AI APT system could gain access to tremendous offensive cyber capability" (p. 19)

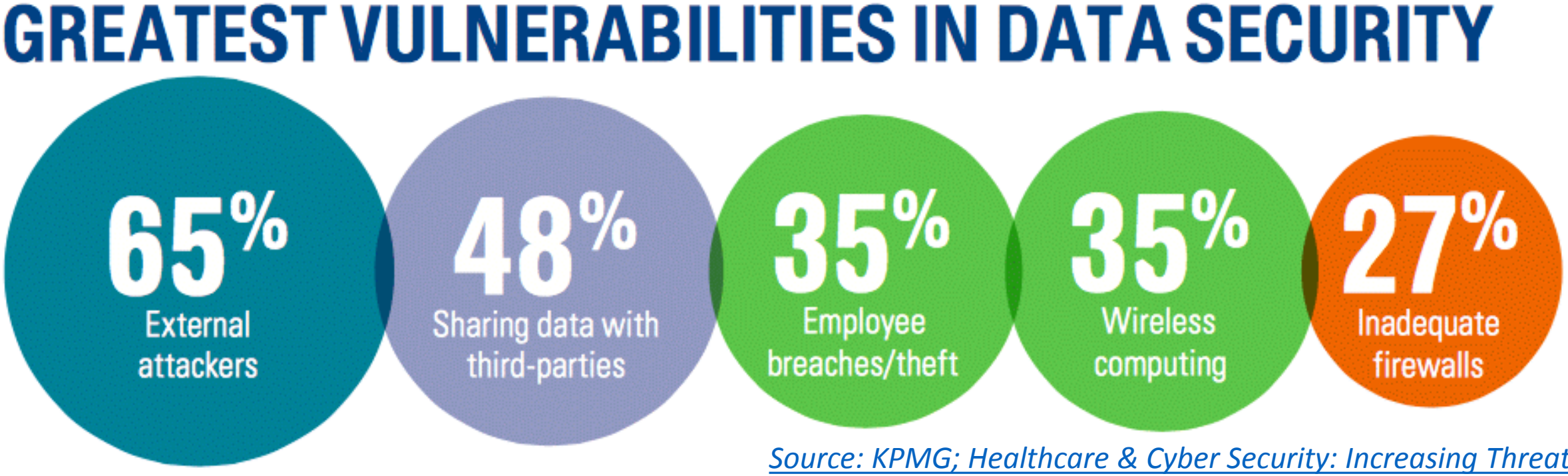
Who are the Hackers?

In the past cyber crime was perpetrated by lone hackers.

Now, the vast majority of attacks come from large, organized crime rings.

- They function like start-ups
- Employ highly trained developers
- Constantly innovating new online attacks called “Zero Day” attacks
- ***No matter how much we do to prevent cyber crime, it is inevitable because of the inherent financial rewards driving bad guys.***

Vulnerability, Threat and Risk



Source: KPMG; Healthcare & Cyber Security: Increasing Threats Require Increased Capabilities.

Common Vulnerabilities

How to Address Vulnerabilities

- Is your data backed up and stored in a secure offsite location? Is restoration tested?
- How is your data being protected if in the cloud?
- How do you control who can access, modify or delete information in your company?
- What kind of antivirus is in use? Is it sufficient for our business? Is it current? Is it running?
- How do we scan for vulnerabilities? How do we monitor suspicious activity or actual attacks?
- Are your employees regularly trained on known threats?
- Is your IT staff or Managed Service Provider (MSP) continually updating their knowledge of security threats and best practices? How do you know they are remaining current?

Types of Threats

Natural threats

- E.g. Flood, fire, tornado, etc.

Unintentional threats

- E.g. Employees accidentally accessing or deleting information, etc.

Intentional threats

- E.g. spyware, malware, adware, disgruntled employees, worms, viruses, etc.

Cyber Risks


Injury or loss of life
Financial loss
Disruption to your business
Loss of privacy
Damage to reputation
Legal implications

Putting it All Together

Risk = Threat + Vulnerability

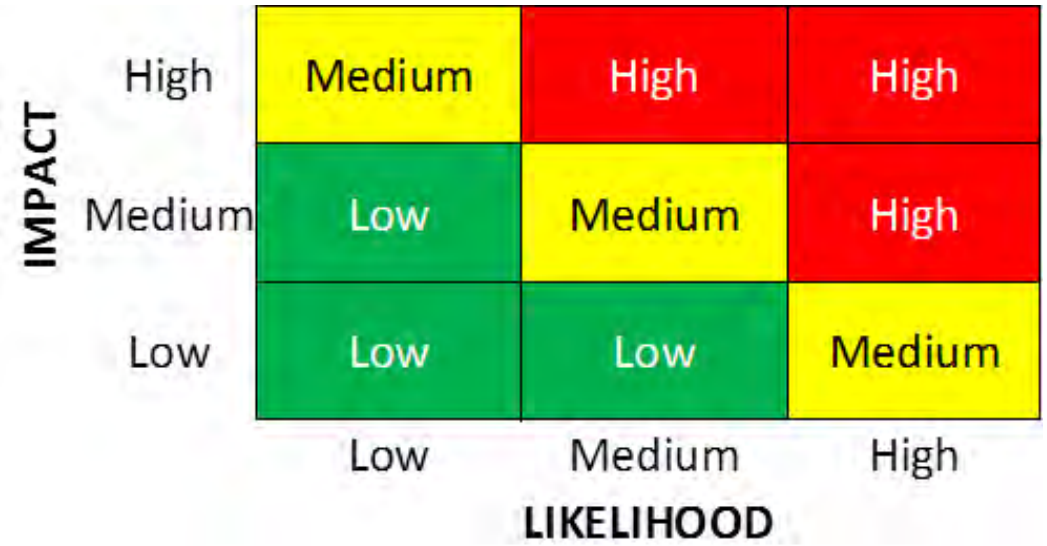
“What happens if a threat exploits a vulnerability?”

Dealing with risk can be done through a risk management plan

Likelihood – What are the chances it could occur?

Impact – How serious would that be?

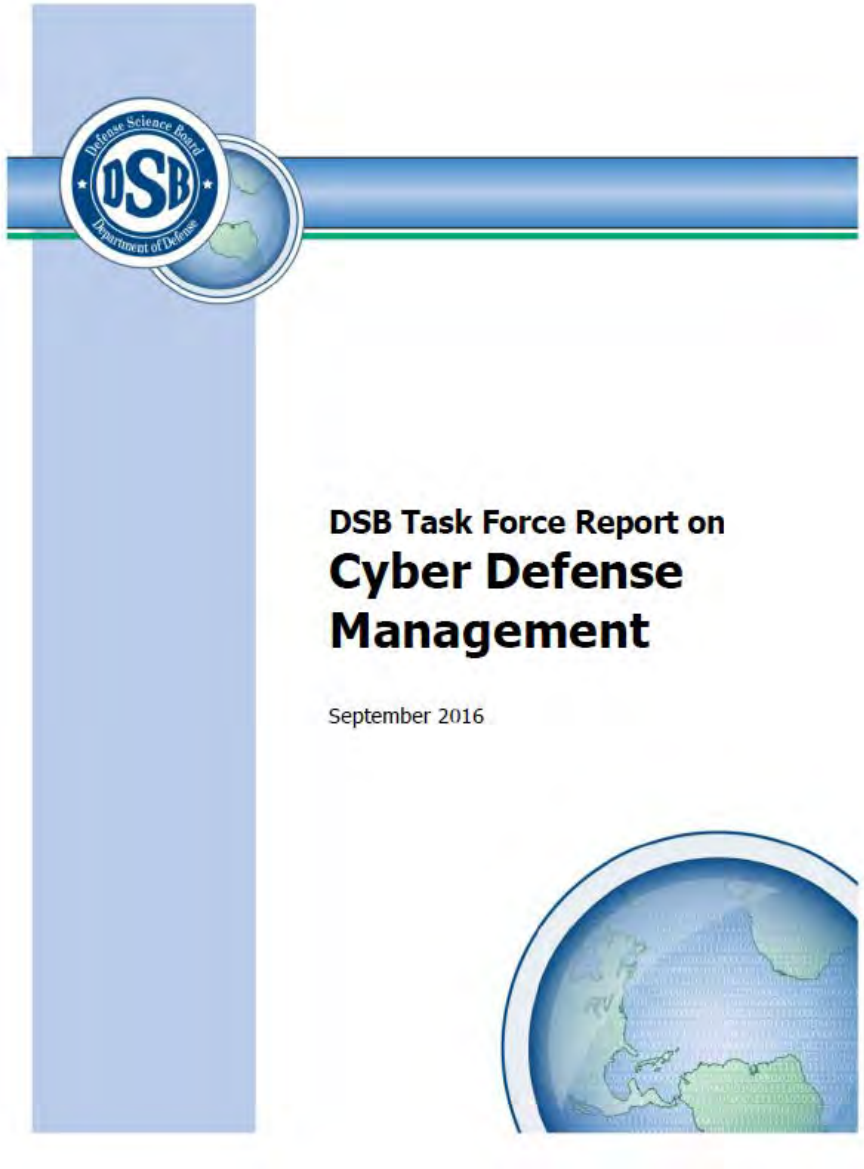
Risk – How important is this?



Risk = Impact x Likelihood

Level of Risk

Treating Risk

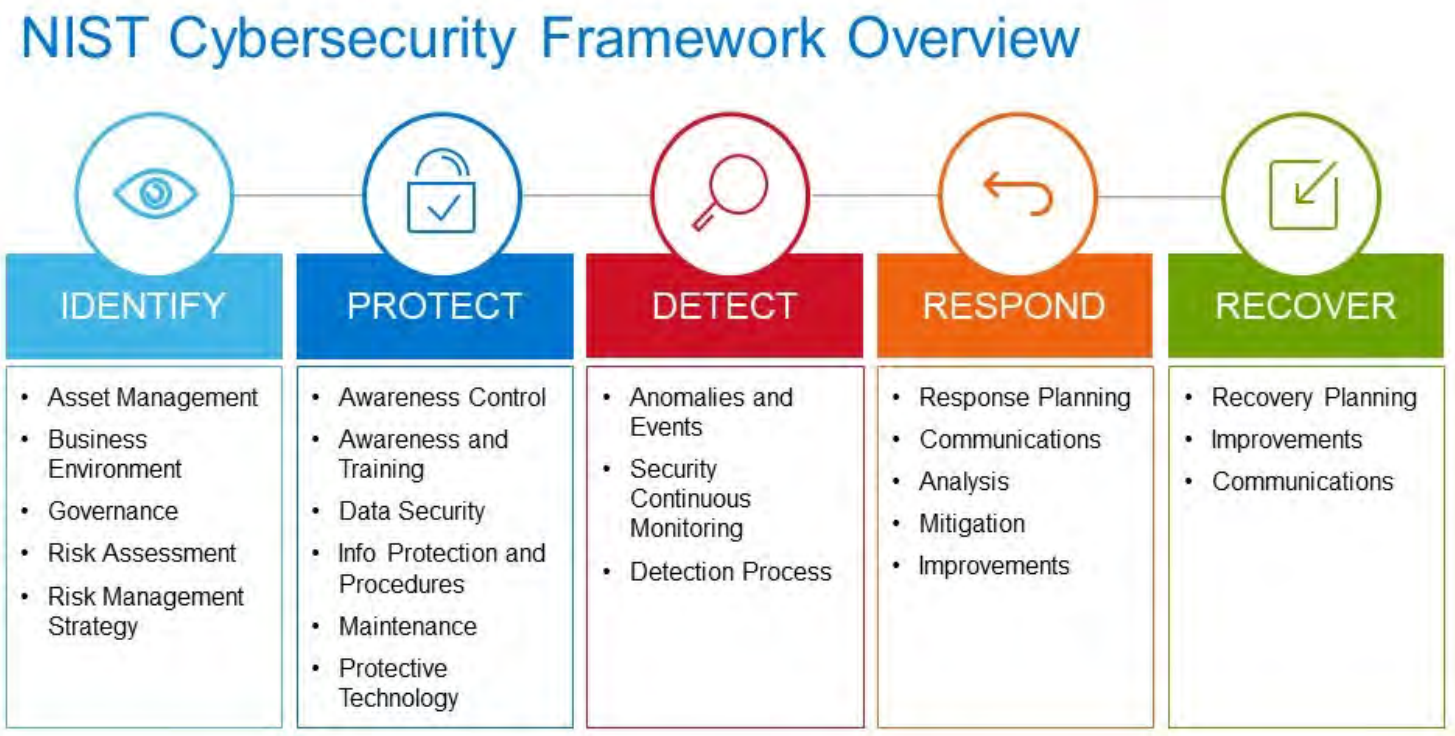


Basic CYBER Investments

- "One of the most important steps for improving the United States' overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves. " (p. 5)

Information Security Control Sets

NIST Cyber Security Framework (CSF)



https://www.nist.gov/cyberframework

An Introduction to Information Security

NIST 800-12

https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final

Control Type	Controls
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessment
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communication Protection

International Organization for Standardization

ISO 27001 Annex A / ISO 27002

https://www.iso.org/isoiec-27001-information-security.html

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resources security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operational security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier Relationships
- A.16 Information security incident management
- A.17 information security aspects of business continuity management
- A.18 Compliance

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://www.cisecurity.org/controls/

DFARS 252.204-7012
NIST 800-171

https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

https://www.aia-aerospace.org/issue/cyber-security/

NAS9933 National Aerospace Standard

1. Device Inventory
2. Software Inventory
3. Secure Configurations
4. Assess/Remediation
5. Malware Defenses
6. In-House SW Security
7. Wireless Access
8. Data Recovery
9. Skills/Training
10. Network Devices
11. Network Controls
12. Administrative Privileges
13. Boundary Defense
14. Audit Logs
15. Controlled Access
16. Account Monitoring and Control
17. Data Protection
18. Incident Management
19. Secure Network Engineering
20. Penetration Tests
21. Governance
22. Mobile Device

AEROSPACE INDUSTRIES ASSOCIATION

NATIONAL AEROSPACE STANDARDS

Common Cybersecurity Myths


MYTH
REALITY
1
*****
A strong password is enough to keep your business safe
Two-factor authentication and data monitoring is also needed

Passwords

Small Businesses


MYTH
REALITY
3
Only certain industries are vulnerable to cyber attacks
Any business with sensitive information is vulnerable to attack

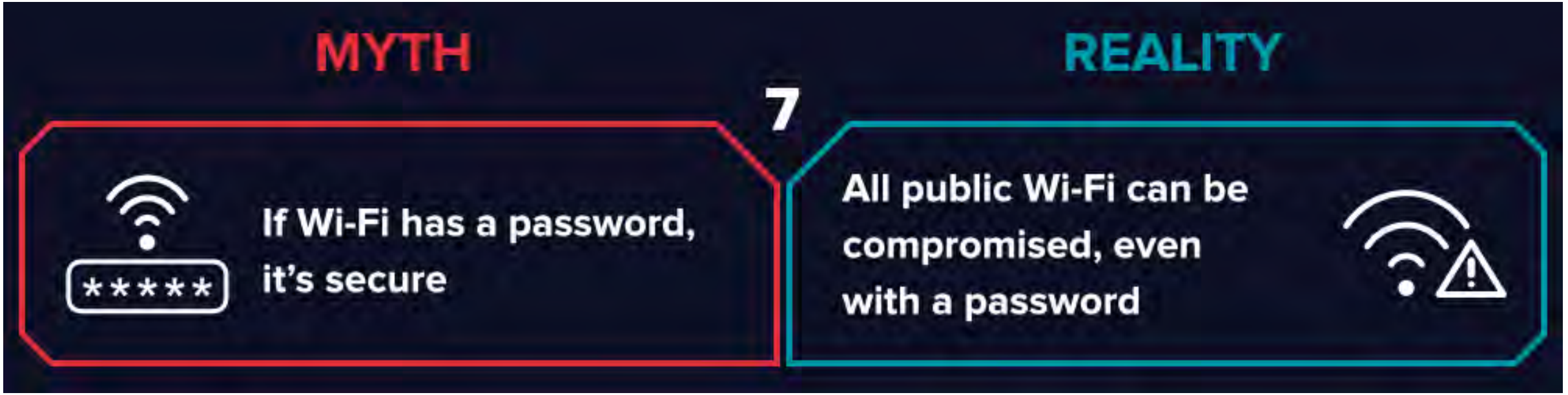
Industry


MYTH
REALITY
4
Anti-virus and anti-malware software keeps you completely safe
Software can't protect against all cyber risks

Software

Insider Threats

Responsibility

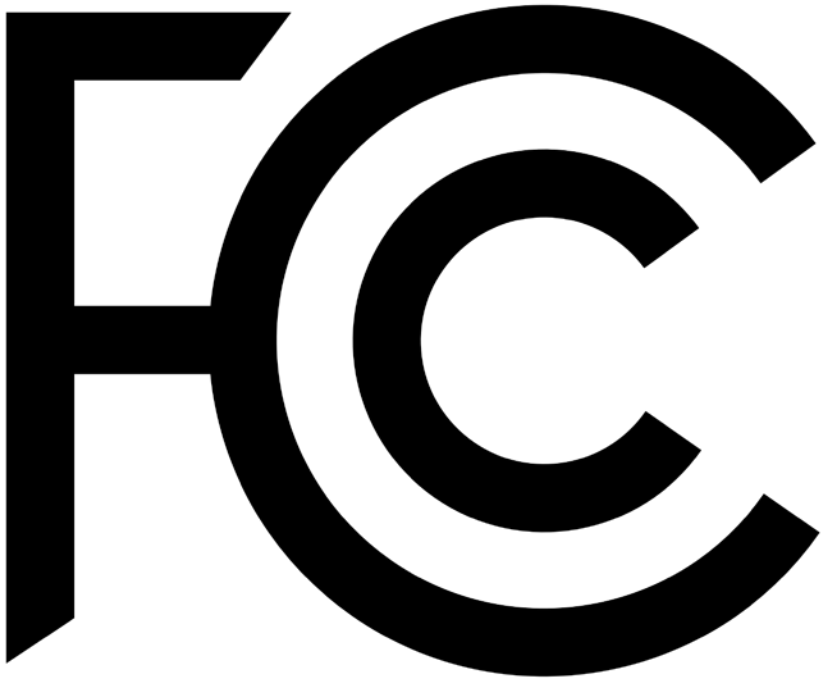


Wi-Fi Security

Delayed Attack

Personal Devices

Complete Security



Ten Cyber Security Tips for Small Businesses

U.S. FCC

https://www.fcc.gov/general/cybersecurity-small-business

1. Train employees in security principles.

2. Protect information, computers, and networks from cyber attacks.

3. Provide firewall security for your Internet connection.

4. Create a mobile device action plan.

5. Make backup copies of important business data and information.

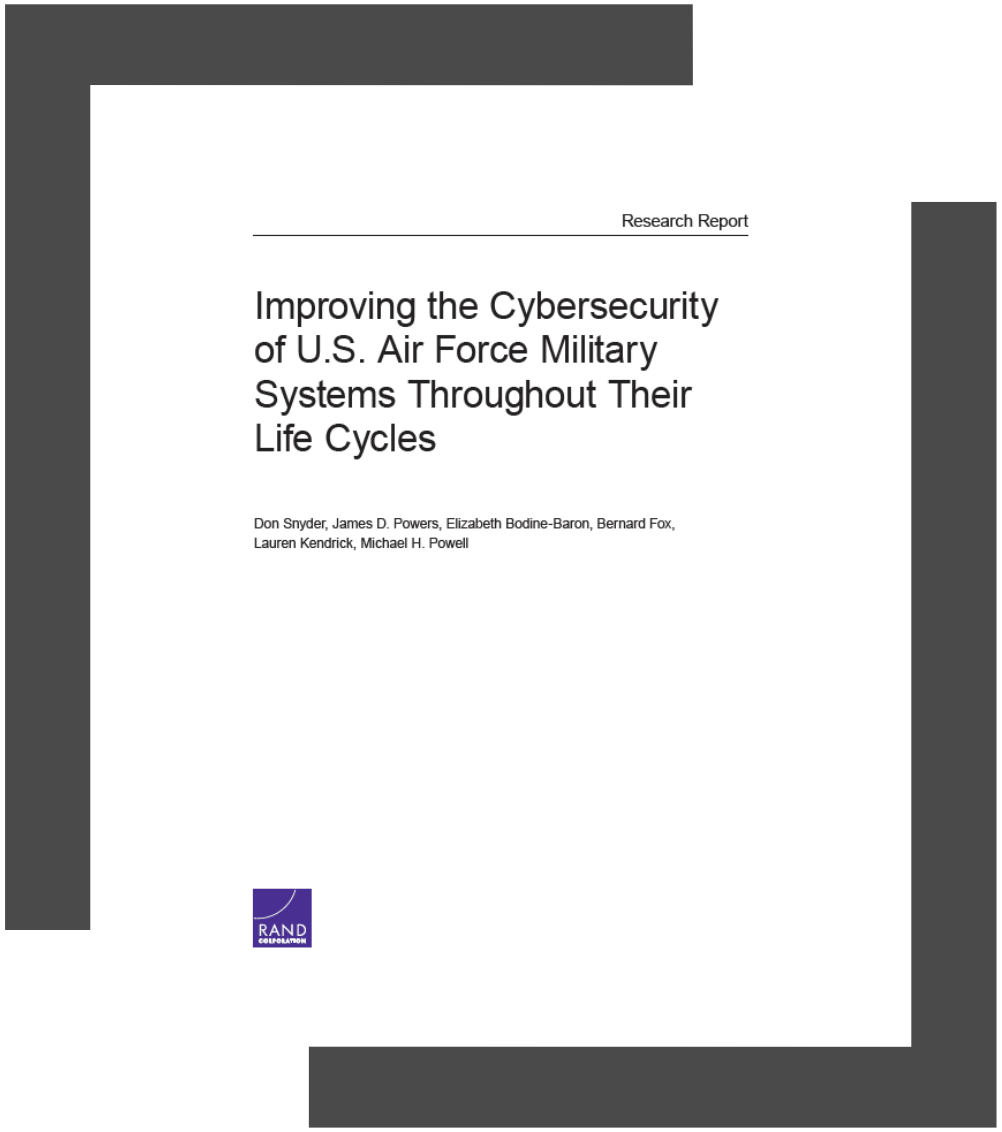
6. Control physical access to your computers and create user accounts for each employee.

7. Secure your Wi-Fi networks.

8. Employ best practices on payment cards.

9. Limit employee access to data and information, and limit authority to install software.

10. Require employees to use unique passwords and change passwords regularly.



How much is enough?

- Imbalance between the offense and defense in the cyber domain implies that it is unwise to assume that complete cybersecurity can be achieved. Some potential vulnerabilities that can be exploited or attacked will always persist. The goals of counter cyber exploitation are, for example, controlling critical information by identifying it, restricting access to it, and preventing its theft. It is not possible to reduce the amount of critical information to zero. Nor does it appear safe to assume that access can be unequivocally denied. The question is how much security is enough given finite resources and mission needs. (Rand, p. 7)

Scott Dawson

Core Business Solutions, Inc.

Lewisburg, PA USA

Contact Info:

scott.dawson@thecoresolution.com

www.thecoresolution.com

866-354-0300

Questions?

Thank You

Scott Dawson

Core Business Solutions, Inc.

Lewisburg, PA USA

Contact Info:

scott.dawson@thecoresolution.com

www.thecoresolution.com

866-354-0300

thecore solution.com
ISO Experts for Small Business