Cybersecurity for Small Business

the fundamentals

Why Cybersecurity Matters for your Small Business

WHY HACKERS HACK

MOTIVES BEHIND CYBERATTACKS

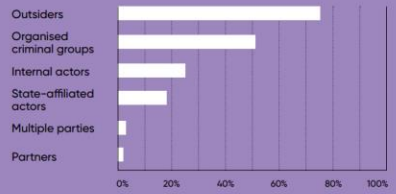
GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK

41%	27%	26%	26%	24%	20%	11%
Ransom	Insider threat	Political	Competition	Cyberwar	Angry user	Motive unknown

Radware 2017

WHO'S BEHIND DATA BREACHES?

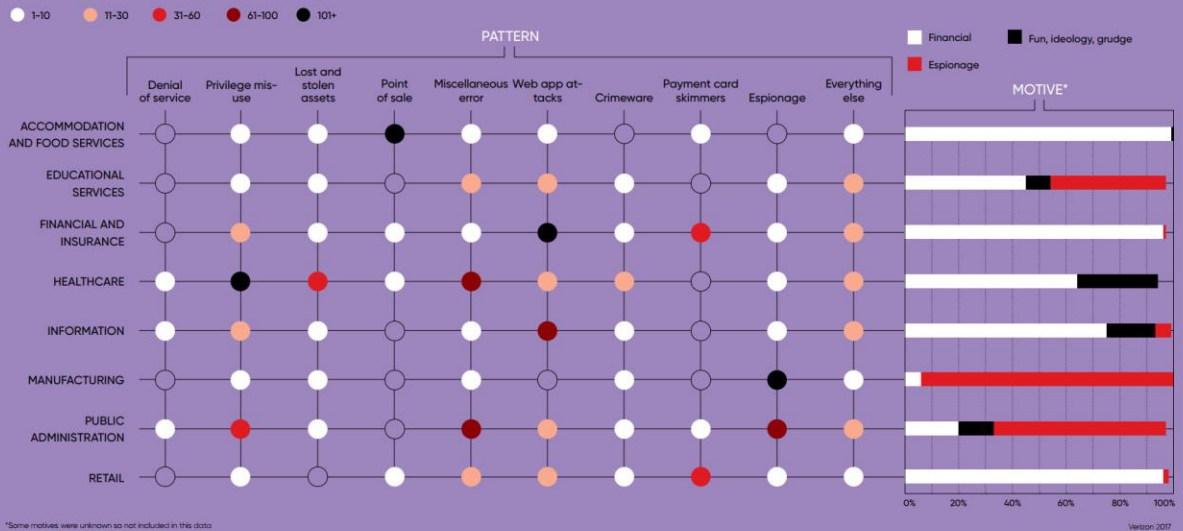
GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



Verizon 2017

DATA BREACHES, BY PATTERN AND MOTIVE

GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES



*Some motives were unknown so not included in this data

Verizon 2017

RACONTEUR

What You'll Learn

- Cybersecurity basics
- Risk management
- Cybersecurity Framework
- Small business cybersecurity resources

More Information
Throughout this presentation, keep an eye out for these boxes which will direct you to publications containing definitions, examples and more related to the topic on the slide.

Cybersecurity Basics

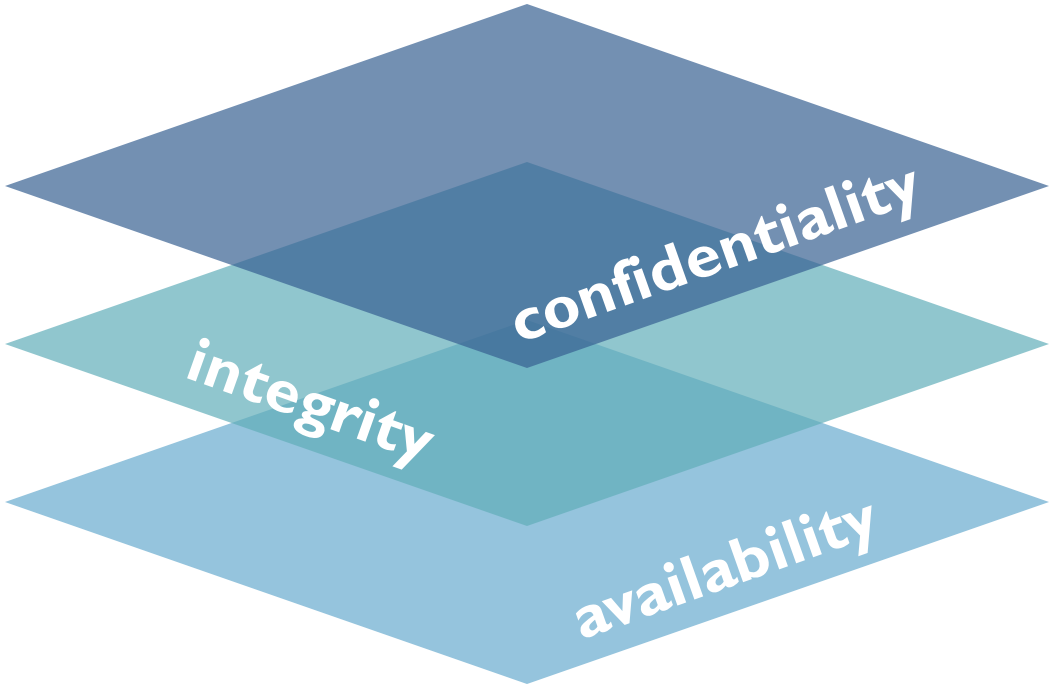
Cybersecurity:

protecting electronic devices and associated data and information

Complexity of a modern small business

- Email
- Mobile devices
- Corporate website
- Social media
- Ecommerce systems
- Online banking
- BYOD and office policy
- Network management
- Backup and remote access

Cybersecurity Objectives

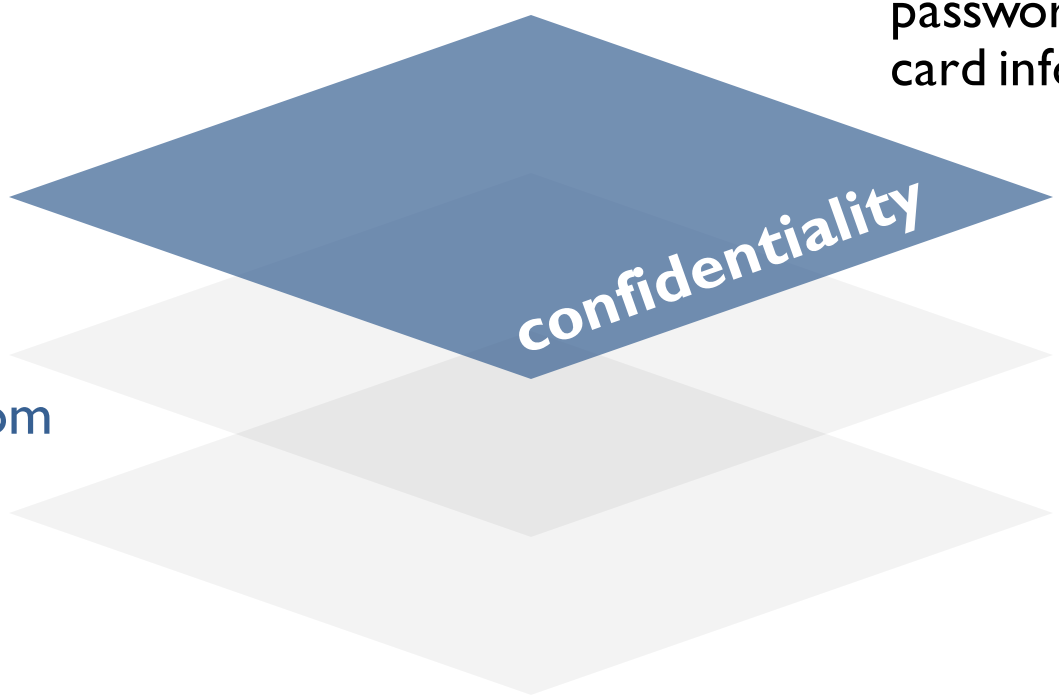


More
NIST Special Publication 800-12, revision 1
An Introduction to Information Security
section 1.4

Confidentiality

Example:

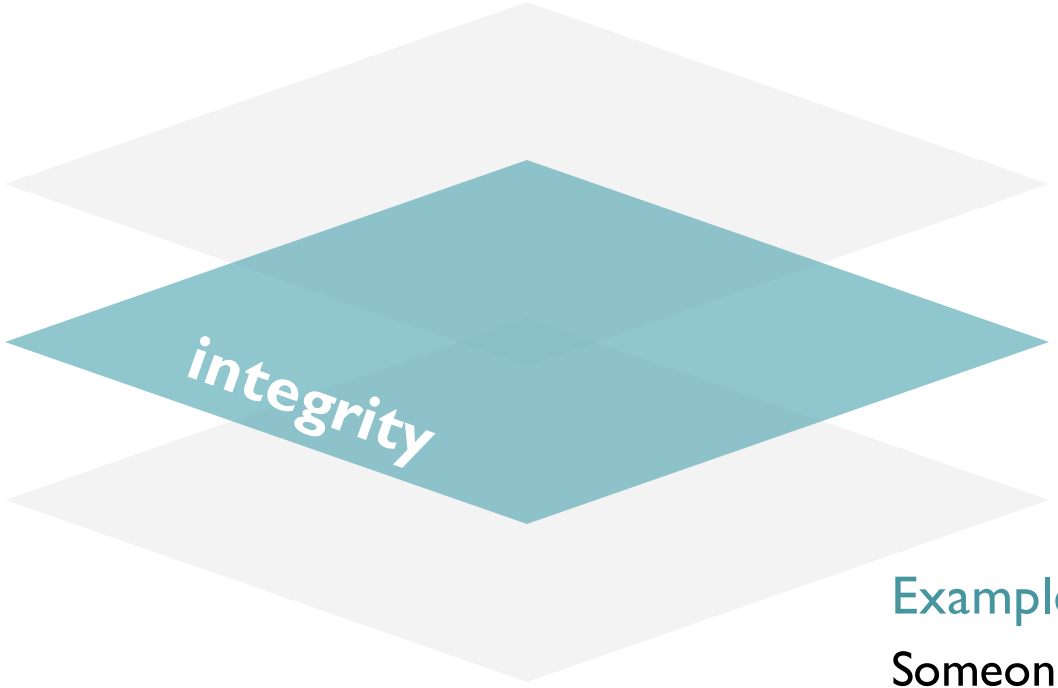
Criminal steals customers' usernames, passwords, or credit card information



Protecting information from unauthorized access and disclosure

Integrity

Protecting information from unauthorized modification



Example:

Someone alters payroll information or a proposed product design

Availability

Example:

Your customers are unable to access your online services

Preventing disruption in how information is accessed

Small Business, Big Impact

Why put your already limited resources into preparing for and protecting against cybersecurity attacks?

Vulnerability	Business Costs	Reputation
Attackers can see small businesses as easy targets	Attacks can be extremely costly and threaten the viability of your business	Customers and employees expect and trust you to keep their information secure

Cybersecurity Basics Resources

Want more details?

For a primer on cybersecurity basics with a focus on small businesses, check out NISTIR 7621, revision 1.

More
NIST Interagency Report 7621, revision 1
Small Business Information Security: The Fundamentals
Section 1: Background: What is Information Security and Cybersecurity?

Cybersecurity Threats

- **Phishing Attacks**
- **Ransomware**
- **Hacking**
- **Imposter Scams**
- **Environmental events**

More
NIST Interagency Report 7621, revision 1 | *Small Business Information Security: The Fundamentals*, section 2.1

Phishing Attacks

- Social engineering attack involving trickery
- Designed to gain access to systems or steal data
- Targeted phishing is "spear phishing"
- Variants include "vishing" – attacks by telephone and "smishing" those using SMS or text

Example:

An email about a delayed shipment causes you to click a link and download malware to your network.

Ransomware

- Type of software with malicious intent and a threat to harm your data
- The author or distributor requires a ransom to undo the damage
- No guarantee the ransom payment will work
- Ransom often needs to be paid in cryptocurrency

Example:

WannaCry was one of the most devastating ransomware attacks in history, affecting several hundred thousand machines and crippling banks, law enforcement agencies, and other infrastructure.

Hacking

- Unauthorized access to systems and information
- Website attack such as DDOS
- Access denied to authorized users
- Stolen funds or intellectual property

Example:

Newspaper kiosk's point-of-sale system was hacked; malware installed. Every customer's credit card information was sent to criminals.

Imposter Scams

- Someone "official" calls or emails to report a crisis situation
- They represent the IRS, a bank, the lottery or technical support
- There will be a sense of urgency and a dire penalty or loss if you don't act

Example:

IRS scams – You receive a phone call claiming to be the IRS, reporting you owe money and need to pay or else get hit with a fine.

Environmental Threats

- Natural threats such as fire, earthquake, flood can cause harm to computers or disrupt business access
- Recovery efforts attract scams such as financial fraud
- Downtime can lose customers, clients who can't wait

Example:

Ellicott City flooding wiped out businesses and their computers

Elements of Risk

What are the **threats**?
What are the **vulnerabilities**?
What is the **likelihood** of a threat exploiting a vulnerability?
What would be the **impact** of this to your business?

> **More**
> NIST Special Publication 800-30, revision 1
> *Guide for Conducting Risk Assessments,* section 2.3.1

What are you protecting?

To practice cybersecurity risk management, you can start with these steps:

1. Identify your business' assets
2. Identify the value of these assets
3. Document the impact to your business of loss or damage to the assets
4. Identify likelihood of loss or harm
5. Prioritize your mitigation activities accordingly

More
NIST Interagency Report 7621, revision 1
Small Business Information Security: The Fundamentals, section 2.2

1. Identify Your Business Assets

List the types of information, processes, important people and technology your business relies upon

- Customer info
- Key employees
- Banking info
- Manufacturing Process
- Proprietary technology

Also consider critical business processes like sales and budgeting.

1. Identify Your Business Assets on the Worksheet (cont.)

- In column 1 of the worksheet, list the assets (e.g., information, people, processes, or technology) that are most important to your business
- Add more rows, if needed

Asset
Patient health information
Devices storing patient information (laptops, server in closet, mobile devices)
Processing patient claims to insurance
Receiving payments from insurance and patients
3rd party email provider

2. Identify the Value of the Assets

Go through each asset type you identified and ask these questions:

- What would happen to my business if this asset was made public?
- What would happen to my business if this asset was damaged or inaccurate?
- What would happen to my business if I/my customers couldn't access this asset?

2. Identify the Asset Values on the Worksheet (cont.)

- Pick an asset value scale that works for you (e.g., low, medium, high or a numerical range like 1-5)

Asset	Value of the Asset
Patient health information	High, due to regulations
Devices storing patient information (laptops, server in closet, mobile devices)	Medium
Processing patient claims to insurance	High
Receiving payments from insurance and patients	High
3rd party email provider	Medium

3. Document the Impact to your Business of Loss/Damage to the Assets

- Consider the impact to your business if each asset were lost, damaged, or reduced in value (e.g., intellectual property revealed to competitors)
- This impact may differ from the asset value determined in step 2.

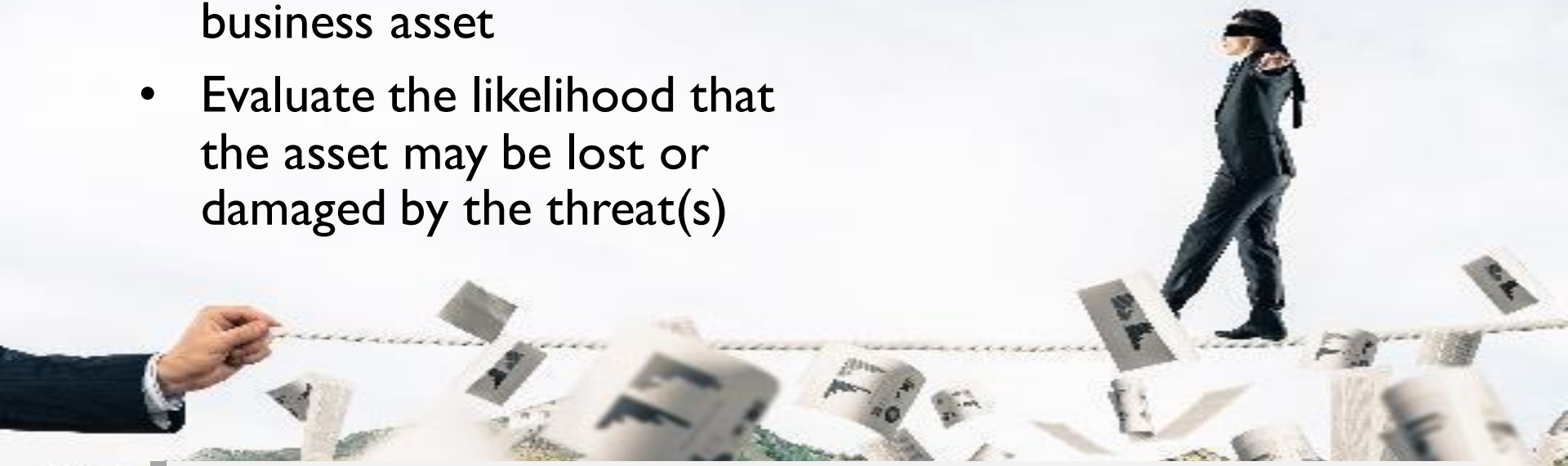
3. Document the Impact to your Business of Loss/Damage to the Assets (cont.)

- Pick an impact value scale that works for you (e.g., low, medium, high)
- Consider if any business processes have manual backup methods

Asset	Value of the Asset	Impact of Loss/ Damage to the Asset
Patient health information	High, due to regulations	**High**
Devices storing patient information (laptops, server in closet, mobile devices)	Medium	**High**
Processing patient claims to insurance	High	**Medium (can institute manual processes temporarily)**
Receiving payments from insurance and patients	High	**High**
3rd party email provider	Medium	**Medium**

4. Identify likelihood of loss or damage to the asset

- List the threats to each business asset
- Evaluate the likelihood that the asset may be lost or damaged by the threat(s)



More
NIST Special Publication 800-30, revision 1
Guide for Conducting Risk Assessments, Appendix G, Likelihood of Occurrence

4. Identify likelihood of loss or damage to the asset (cont.)

Asset	Value of the Asset	Impact of Loss/ Damage to the Asset	Threats to the Asset	Likelihood of Loss/Damage to the Asset
Patient health information	High, due to regulations	High	Hackers, ransomware	Medium
Devices storing patient information (laptops, server in closet, mobile devices)	Medium	High	Thieves, malware, phishing	Low
Processing patient claims to insurance	High	Medium (can institute manual processes temporarily)	Denial of service, hackers	Low
Receiving payments from insurance and patients	High	High	Denial of service, hackers	Low
3rd party email provider	Medium	Medium	Phishing, malware	Medium

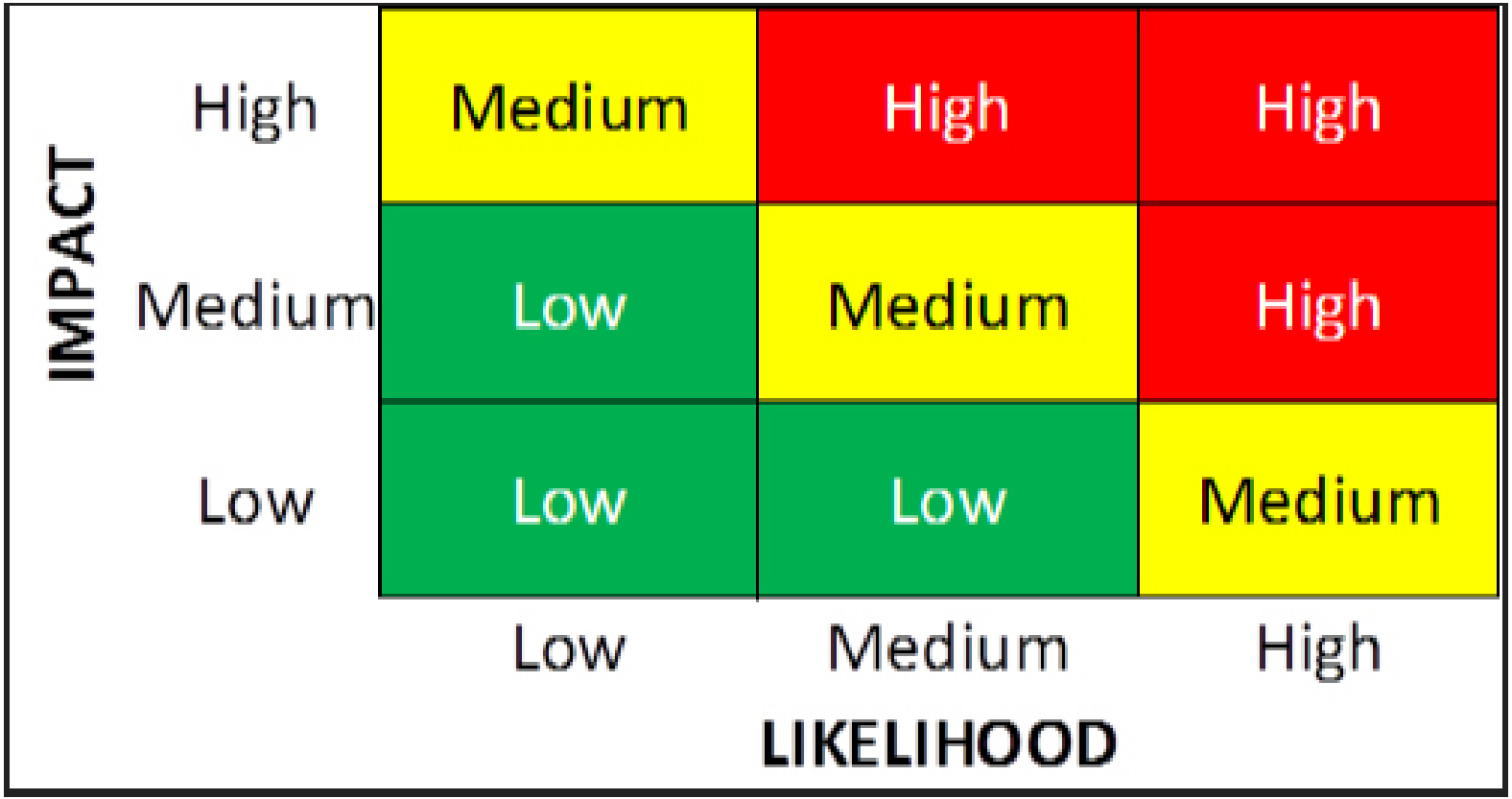
5. Identify Priorities and Potential Solutions

- Compare your impact and likelihood scores. Assets with high impact and/or likelihood scores should be assigned top priorities.
- Identify your priorities.
- Identify potential solutions.
- Develop a plan, including funding, to implement the solutions.

Sample Priority Structure

High: Implement immediate resolution.
Medium: Schedule a resolution.
Low: Schedule a resolution.

5. Prioritize Assets - Risk Matrix



5. Prioritize Asset Protection

Asset	Value of the Asset	Impact of Loss/ Damage to the Asset	Threats to the Asset	Likelihood of Loss/Damage to the Asset	Prioritization of Protection to the Asset
Patient health information	High, due to regulations	High	Hackers, ransomware	Medium	High
Devices storing patient information (laptops, server in closet, mobile devices)	Medium	High	Thieves, malware, phishing	Low	Low
Processing patient claims to insurance	High	Medium **(can institute manual processes temporarily)**	Denial of service, hackers	Low	Low
Receiving payments from insurance and patients	High	High	Denial of service, hackers	Low	Low
3rd party email provider	Medium	Medium	Phishing, malware	Medium	Medium

NIST Cybersecurity Framework ("Framework for Improving Critical Infrastructure Cybersecurity ")

Provides a continuous process for cybersecurity risk management

For organizations of any size, in any sector, whether they have a cyber risk management program already or not

Has proven useful to a variety of audiences

More
Framework for Improving Critical Infrastructure Cybersecurity version 1.1

Cybersecurity Framework Functions

Credit: N. Hanacek/NIST

Identify

Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Sample Identify Activities

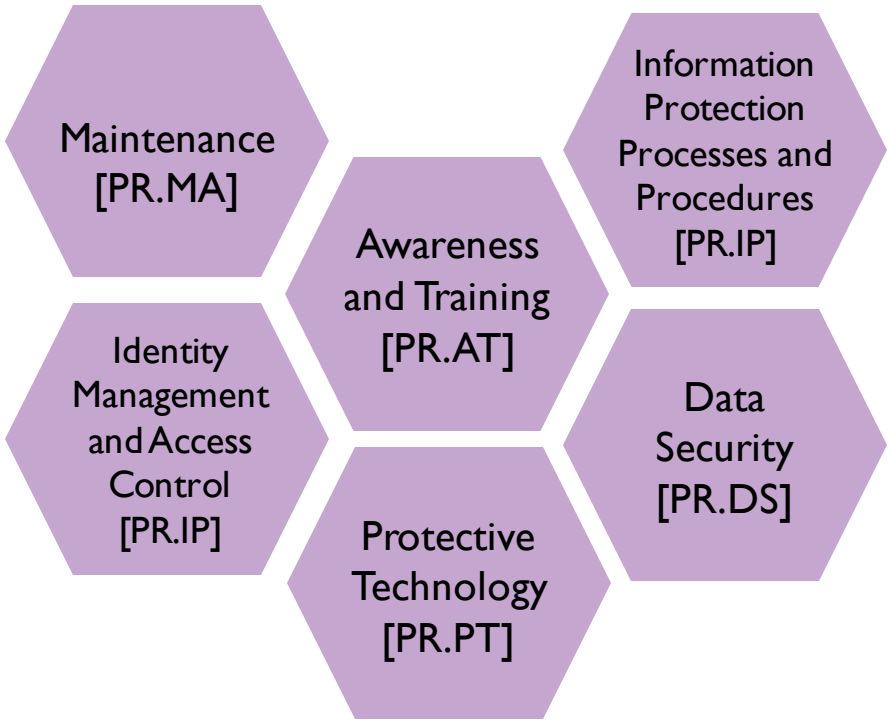
- Business Environment [ID.BE]
- Asset Management [ID.AM]
- Governance [ID.GV]
- Risk Assessment [ID.RA]

- Identify critical business processes
- Document Information flows
- Establish policies for cybersecurity that includes roles and responsibilities
- Maintain hardware and software inventory
- Identify contracts with external partners
- Identify Risk Management processes

Protect

Develop and implement the appropriate safeguards to ensure delivery of services.

Sample Protect Activities



- Manage access to assets and information
- Conduct regular backups
- Protect sensitive data
- Patch operating systems and applications
- Create response and recovery plans
- Protect your network
- Train your employees

Detect

Develop and implement the appropriate activities to **identify the occurrence of a cybersecurity event.**

Sample Detect Activities

Anomalies and Events [DE.AE]

Continuous Monitoring [DE.CM]

- Install and update anti-virus and other malware detection software
- Know what are expected data flows for your business
- Maintain and monitor logs

Respond

Develop and implement the appropriate activities to **take action regarding a detected cybersecurity event.**

Sample Respond Activities

Response Planning [RS.RP]

Communications [RS.CO]

- Coordinate with internal and external stakeholders
- Ensure response plans are tested
- Ensure response plans are updated

Recover

Develop and implement the appropriate activities to maintain plans for **resilience and to restore any capabilities or services** that were impaired due to a cybersecurity event.

Sample Recover Activities

Recovery Planning [RC.RP]

Communications [RC.CO]

- Manage public relations and company reputation
- Communicate with internal and external stakeholders
- Ensure recovery plans are updated
- Consider cyber insurance

Asset Management [ID.AM]

Risk Assessment [ID.RA]

Governance [ID.GV]

Business Environment [ID.BE]

Information Protection Processes and Procedures [PR.IP]

Identity Management and Access Control [PR.IP]

Protective Technology [PR.PT]

Maintenance [PR.MA]

Awareness and Training [PR.AT]

Data Security [PR.DS]

Anomalies and Events [DE.AE]

Continuous Monitoring [DE.CM]

Communications [RS.CO]

Response Planning [RS.RP]

Recovery Planning [RC.RP]

Communications [RC.CO]

Everyday Tips

- Be careful of email attachments, web links and voice calls from unknown numbers.
- Do not click on a link or open an attachment that you were not expecting.
- Use separate personal and business computers, mobile devices, and accounts.
- Use multi-factor authentication where offered.
- Do not download software from an unknown web page.
- Never give out your username or password.
- Consider using a password management application to store your passwords for you.

> **More**
> NIST Interagency Report 7621, revision 1
> *Small Business Information Security: The Fundamentals*, section 4

Need Help?

You might choose to outsource some of your security needs.

- **Ask for recommendations** from business partners, local Chamber of Commerce, Better Business Bureau, colleges or universities.
- **Request quotes** and have a clear list of actions or outcomes that you want to achieve.
- **Check past performance** using reviews posted online. Check for Better Business Bureau or Federal Trade Commission complaints.
- **Find out who will be doing the work** and ask for their qualifications.

> **More**
> NIST Interagency Report 7621, revision 1
> *Small Business Information Security: The Fundamentals*, section 2.3

Resources

NIST Small Business Cybersecurity Corner

https://www.nist.gov/itl/smallbusinesscyber

CyberSecure My Business | National Cyber Security Alliance

https://staysafeonline.org/cybersecure-business/

NIST Interagency Report 7621, revision 1 | *Small Business Information Security: The Fundamentals*

https://doi.org/10.6028/NIST.IR.7621r1

More Information

https://www.nist.gov/itl/smallbusinesscyber

www.NIST.gov/topics/cybersecurity

@NISTcyber

smallbizsecurity@nist.gov