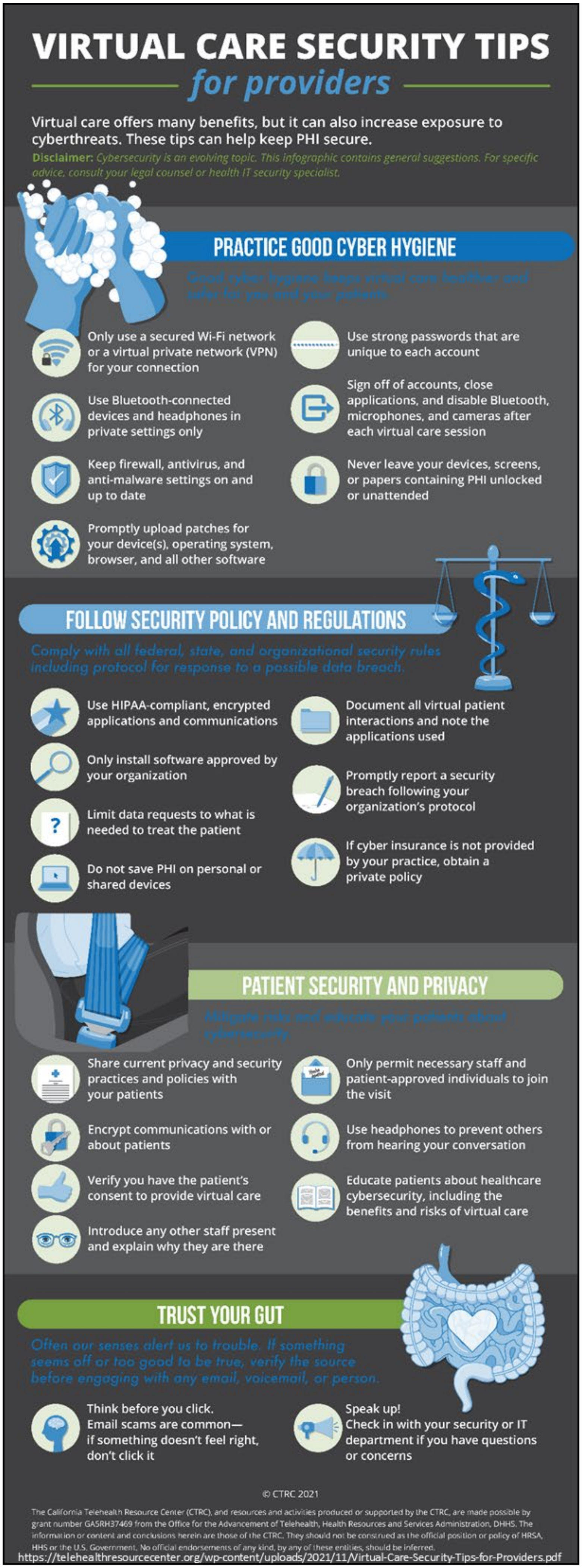


# VIRTUAL CARE SECURITY TIPS
## *for providers*

Virtual care offers many benefits, but it can also increase exposure to cyberthreats. These tips can help keep PHI secure.

**Disclaimer:** *Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.*

### PRACTICE GOOD CYBER HYGIENE

*Good cyber hygiene keeps virtual care healthier and safer for you and your patients.*

- Only use a secured Wi-Fi network or a virtual private network (VPN) for your connection
- Use Bluetooth-connected devices and headphones in private settings only
- Keep firewall, antivirus, and anti-malware settings on and up to date
- Promptly upload patches for your device(s), operating system, browser, and all other software
- Use strong passwords that are unique to each account
- Sign off of accounts, close applications, and disable Bluetooth, microphones, and cameras after each virtual care session
- Never leave your devices, screens, or papers containing PHI unlocked or unattended

### FOLLOW SECURITY POLICY AND REGULATIONS

*Comply with all federal, state, and organizational security rules including protocol for response to a possible data breach.*

- Use HIPAA-compliant, encrypted applications and communications
- Only install software approved by your organization
- Limit data requests to what is needed to treat the patient
- Do not save PHI on personal or shared devices
- Document all virtual patient interactions and note the applications used
- Promptly report a security breach following your organization's protocol
- If cyber insurance is not provided by your practice, obtain a private policy

### PATIENT SECURITY AND PRIVACY

*Mitigate risks and educate your patients about cybersecurity.*

- Share current privacy and security practices and policies with your patients
- Encrypt communications with or about patients
- Verify you have the patient's consent to provide virtual care
- Introduce any other staff present and explain why they are there
- Only permit necessary staff and patient-approved individuals to join the visit
- Use headphones to prevent others from hearing your conversation
- Educate patients about healthcare cybersecurity, including the benefits and risks of virtual care

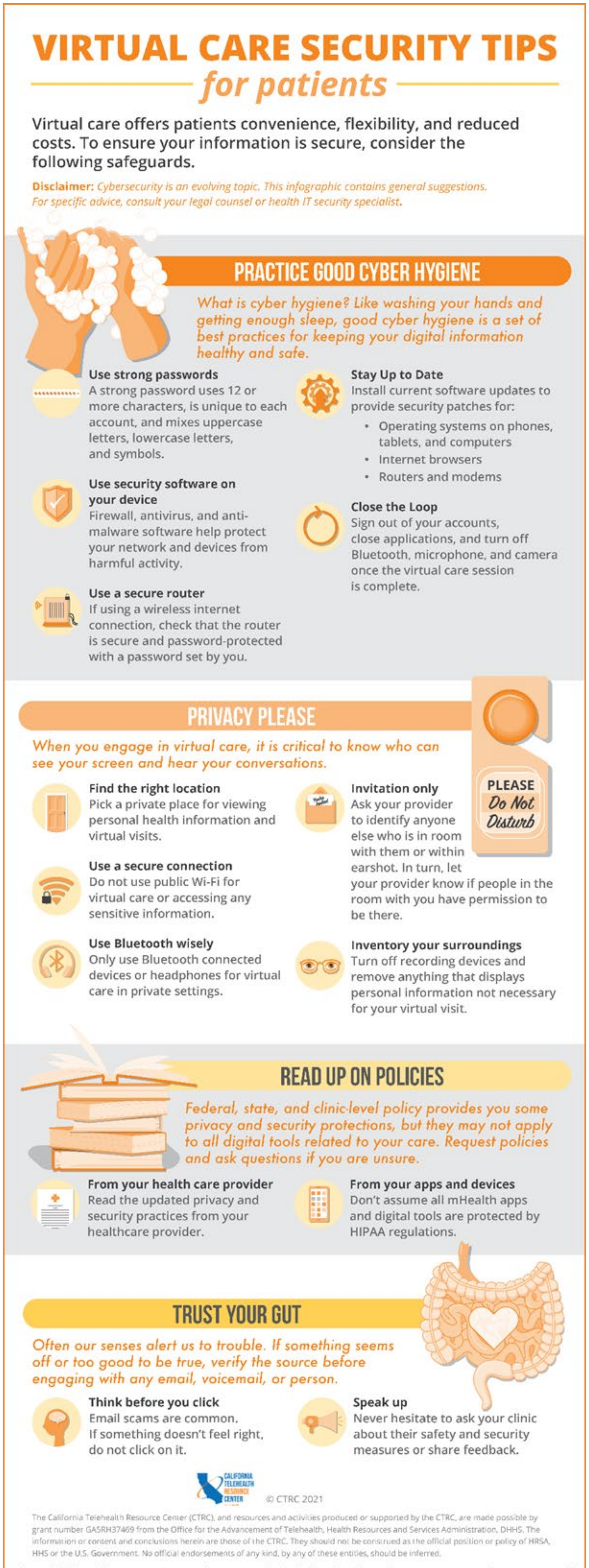
### TRUST YOUR GUT

*Often our senses alert us to trouble. If something seems off or too good to be true, verify the source before engaging with any email, voicemail, or person.*

- Think before you click. Email scams are common—if something doesn't feel right, don't click it
- Speak up! Check in with your security or IT department if you have questions or concerns

The California Telehealth Resource Center (CTRC), and resources and activities produced or supported by the CTRC, are made possible by grant number GA5RH37469 from the Office for the Advancement of Telehealth, Health Resources and Services Administration, DHHS. The information or content and conclusions herein are those of the CTRC. They should not be construed as the official position or policy of HRSA, HHS or the U.S. Government. No official endorsements of any kind, by any of these entities, should be inferred.

https://telehealthresourcecenter.org/wp-content/uploads/2021/11/Virtual-Care-Security-Tips-for-Providers.pdf



# VIRTUAL CARE SECURITY TIPS
## *for patients*

Virtual care offers patients convenience, flexibility, and reduced costs. To ensure your information is secure, consider the following safeguards.

**Disclaimer:** *Cybersecurity is an evolving topic. This infographic contains general suggestions. For specific advice, consult your legal counsel or health IT security specialist.*

### PRACTICE GOOD CYBER HYGIENE

*What is cyber hygiene? Like washing your hands and getting enough sleep, good cyber hygiene is a set of best practices for keeping your digital information healthy and safe.*

**Use strong passwords**
A strong password uses 12 or more characters, is unique to each account, and mixes uppercase letters, lowercase letters, and symbols.

**Use security software on your device**
Firewall, antivirus, and anti-malware software help protect your network and devices from harmful activity.

**Use a secure router**
If using a wireless internet connection, check that the router is secure and password-protected with a password set by you.

**Stay Up to Date**
Install current software updates to provide security patches for:

- Operating systems on phones, tablets, and computers
- Internet browsers
- Routers and modems

**Close the Loop**
Sign out of your accounts, close applications, and turn off Bluetooth, microphone, and camera once the virtual care session is complete.

### PRIVACY PLEASE

PLEASE *Do Not Disturb*

*When you engage in virtual care, it is critical to know who can see your screen and hear your conversations.*

**Find the right location**
Pick a private place for viewing personal health information and virtual visits.

**Use a secure connection**
Do not use public Wi-Fi for virtual care or accessing any sensitive information.

**Use Bluetooth wisely**
Only use Bluetooth connected devices or headphones for virtual care in private settings.

**Invitation only**
Ask your provider to identify anyone else who is in room with them or within earshot. In turn, let your provider know if people in the room with you have permission to be there.

**Inventory your surroundings**
Turn off recording devices and remove anything that displays personal information not necessary for your virtual visit.

### READ UP ON POLICIES

*Federal, state, and clinic-level policy provides you some privacy and security protections, but they may not apply to all digital tools related to your care. Request policies and ask questions if you are unsure.*

**From your health care provider**
Read the updated privacy and security practices from your healthcare provider.

**From your apps and devices**
Don't assume all mHealth apps and digital tools are protected by HIPAA regulations.

### TRUST YOUR GUT

*Often our senses alert us to trouble. If something seems off or too good to be true, verify the source before engaging with any email, voicemail, or person.*

**Think before you click**
Email scams are common. If something doesn't feel right, do not click on it.

**Speak up**
Never hesitate to ask your clinic about their safety and security measures or share feedback.

CALIFORNIA TELEHEALTH RESOURCE CENTER

The California Telehealth Resource Center (CTRC), and resources and activities produced or supported by the CTRC, are made possible by grant number GA5RH37469 from the Office for the Advancement of Telehealth, Health Resources and Services Administration, DHHS. The information or content and conclusions herein are those of the CTRC. They should not be construed as the official position or policy of HRSA, HHS or the U.S. Government. No official endorsements of any kind, by any of these entities, should be inferred.

https://telehealthresourcecenter.org/wp-content/uploads/2022/12/Virtual-Care-Security-Tips-for-Patients-2.pdf

# Privacy and Cybersecurity for Healthcare Organizations

## The NIST Cybersecurity Framework (CSF) 2.0

**GOVERN**
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

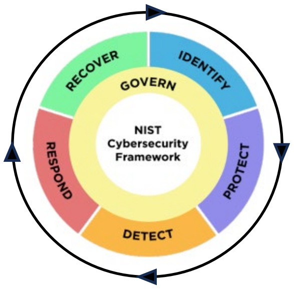
**IDENTIFY**
The organization's current cybersecurity risks are understood.

**PROTECT**
Safeguards to manage the organization's cybersecurity risks are used.

**DETECT**
Possible cybersecurity attacks and compromises are found and analyzed.

**RESPOND**
Actions regarding a detected cybersecurity incident are taken.

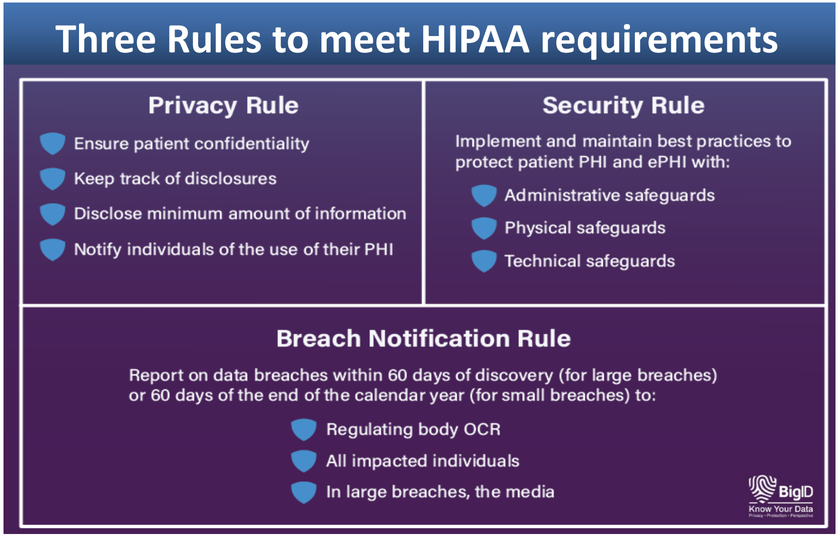
**RECOVER**
Assets and operations affected by a cybersecurity incident are restored.



Figures adapted from NIST publications: NIST.SP.1299.pdf and NIST.CSWP.29.pdf

| Function | Category |
|---|---|
| **Govern (GV)** | Organizational Context |
| | Risk Management Strategy |
| | Roles, Responsibilities, and Authorities |
| | Policy |
| | Oversight |
| | Cybersecurity Supply Chain Risk Management |
| **Identify (ID)** | Asset Management |
| | Risk Assessment |
| | Improvement |
| **Protect (PR)** | Identity Management, Authentication, and Access Control |
| | Awareness and Training |
| | Data Security |
| | Platform Security |
| | Technology Infrastructure Resilience |
| **Detect (DE)** | Continuous Monitoring |
| | Adverse Event Analysis |
| **Respond (RS)** | Incident Management |
| | Incident Analysis |
| | Incident Response Reporting and Communication |
| | Incident Mitigation |
| **Recover (RC)** | Incident Recovery Plan Execution |
| | Incident Recovery Communication |

## Health Information Privacy



### Three Rules to meet HIPAA requirements

**Privacy Rule**

- Ensure patient confidentiality
- Keep track of disclosures
- Disclose minimum amount of information
- Notify individuals of the use of their PHI

**Security Rule**

Implement and maintain best practices to protect patient PHI and ePHI with:

- Administrative safeguards
- Physical safeguards
- Technical safeguards

**Breach Notification Rule**

Report on data breaches within 60 days of discovery (for large breaches) or 60 days of the end of the calendar year (for small breaches) to:

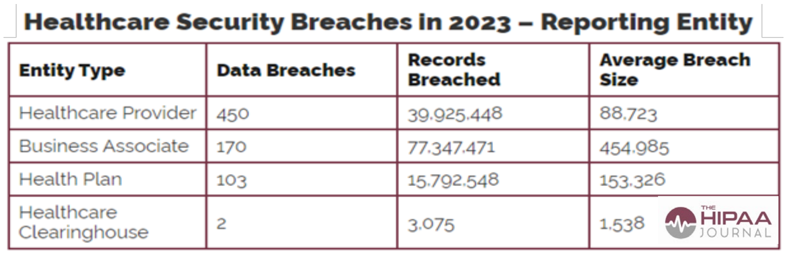
- Regulating body OCR
- All impacted individuals
- In large breaches, the media

BigID Know Your Data

Collecting, Using, or Sharing Consumer Health Information?

Look to HIPAA, the FTC Act, and the Health Breach Notification Rule

| Key Patient and Consumer Health Information Privacy Laws | Key Protected Health Information Privacy Risks | Key Protected Health Information Privacy Breach Causes |
|---|---|---|
| FTC Act 1914 | Hacking/IT Incidents | Human Behavior: Error, Social Engineering, Privilege Misuse, Insider Threats |
| HIPAA 1996 | Unauthorized Access/Disclosure | Business Email Compromise: Phishing |
| COPPA 1998 | Loss/Theft | Ransomware |
| HITECH Act 2009 | Improper Disposal | IT System Misconfiguration |
| HIPAA Omnibus Rule 2013 | | Failure to assess and manage risk |
| State privacy laws that exceed, but are not contrary to, federal privacy laws | | Sharing PHI with 3rd parties/vendors without a BAA and without vetting information security practices |
| | | Exploitation of software and hardware vulnerabilities |
| | | Loss or Theft of Unencrypted Data |
| | | Lack of / insufficient training |



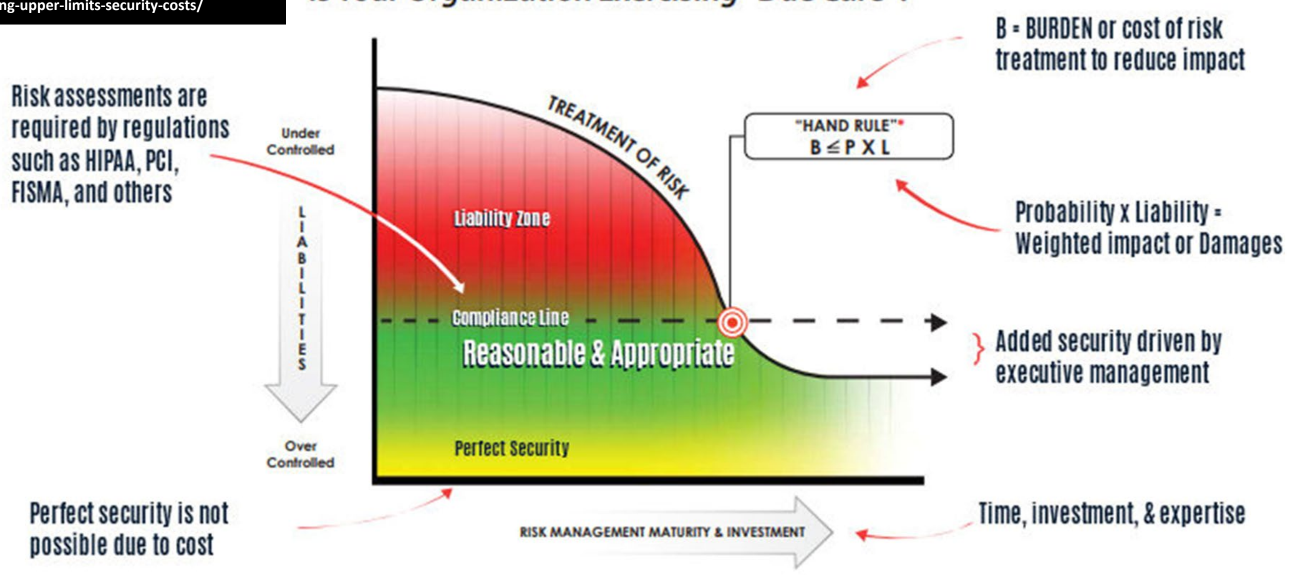
### Healthcare Security Breaches in 2023 – Reporting Entity

| Entity Type | Data Breaches | Records Breached | Average Breach Size |
|---|---|---|---|
| Healthcare Provider | 450 | 39.925.448 | 88.723 |
| Business Associate | 170 | 77.347.471 | 454.985 |
| Health Plan | 103 | 15.792.548 | 153.326 |
| Healthcare Clearinghouse | 2 | 3.075 | 1.538 |

THE HIPAA JOURNAL

Source: https://www.halock.com/hand-rule-managing-upper-limits-security-costs/

*Is Your Organization Exercising "Due Care"?*



Risk assessments are required by regulations such as HIPAA, PCI, FISMA, and others

B = BURDEN or cost of risk treatment to reduce impact

Probability x Liability = Weighted impact or Damages

Added security driven by executive management

Perfect security is not possible due to cost

Time, investment, & expertise

**Source references and additional resources available via QR code/ URL below**

https://tinyurl.com/bdex9cza