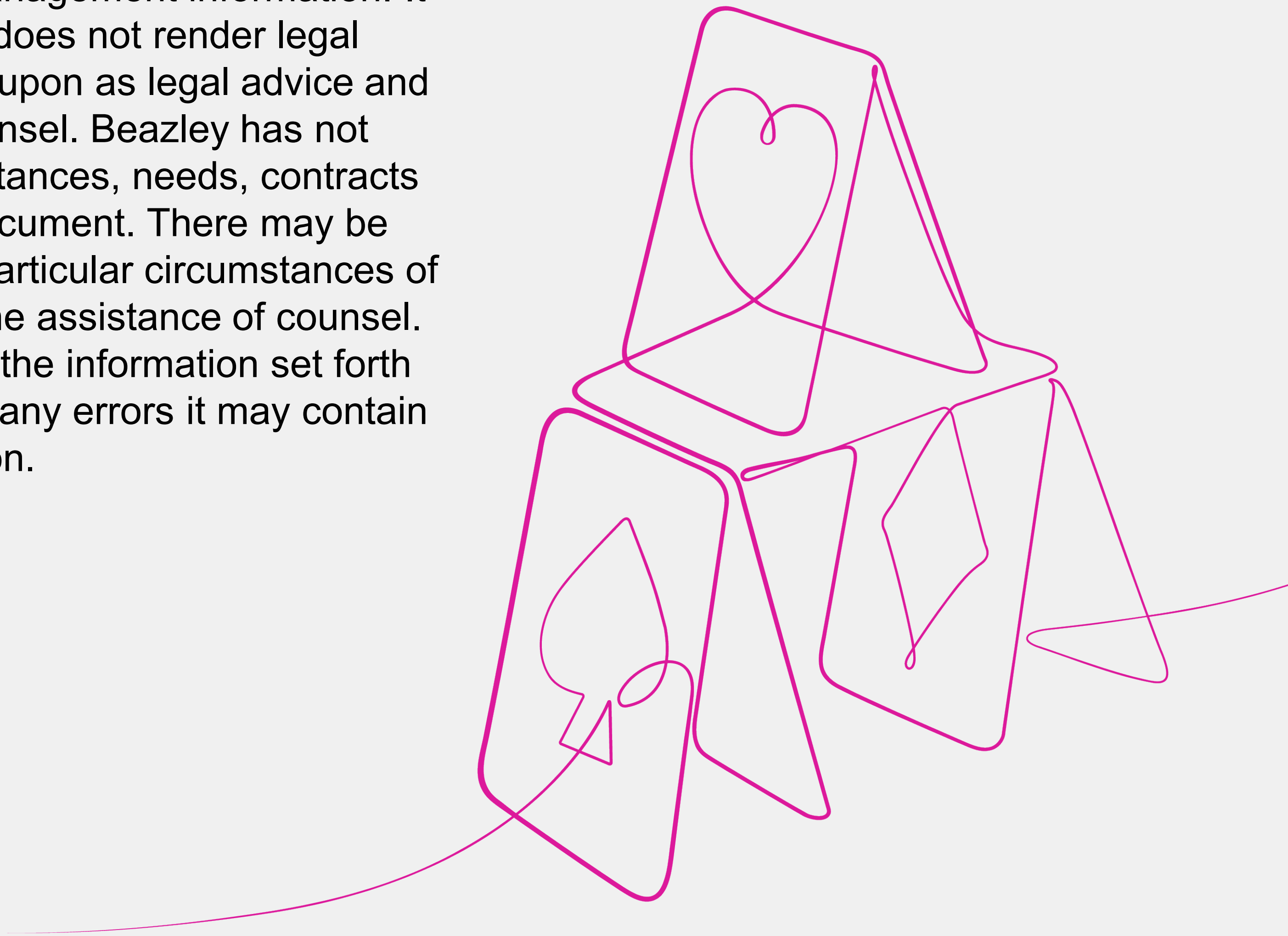
2024 Healthcare Cybersecurity Trends and Tips

KAMMCO Webinar
Presented by Beazley

beazley

Disclaimer:

The information set forth is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.



With you today:

Henri-Errol Smith

Claims Manager
Cyber & Tech - Treaty &
Beazley Product Solutions (BPS) Claims

Email: henri-errol.smith@beazley.com

Why Is The Healthcare Industry a Top Target?

- **Data rich environments** – lots of data held and rarely removed
  - Regulatory requirements
  - Ongoing studies/research
- **Ransomware Target**
  - 24/7 Operations
  - Sensitive data that is in high demand
- **Very Open Environment** – Caregivers have access to medical records across various platforms
- **Healthcare cybersecurity can be less mature**
- **Large gaps**

Further Healthcare Security Insights

Irregular Environments

- Environments can be wide-reaching
- Inconsistent levels of cyber investment
- Unequal budgets – small, rural clinic vs cutting-edge hospital

Regulation up to Interpretation

- HIPAA is very important, but language can leave room for interpretation
- A large portion of healthcare entities only have basic detection and response capabilities

Time Poor and High Risk

- Difficulties unique to HC
- Challenges with finding time to train medical professionals on new security measures
- Doctors not pleased with prospect of taking more time to enter in longer passwords, etc.

Legacy Systems

- Older systems and programs can be crucial to operating medical equipment
- Replacing legacy systems can mean replacing the entirety of the medical equipment

Regulatory Implications & HIPAA

- **Security Rules under HIPAA**
  - Risk analysis
  - Risk management plan
  - Appropriate security safeguards
  - Disaster recovery and business continuity plans
- **Office for Civil Rights**
  - Investigations
  - Enforcement
  - Recognized security practices
- **State Law Requirements**

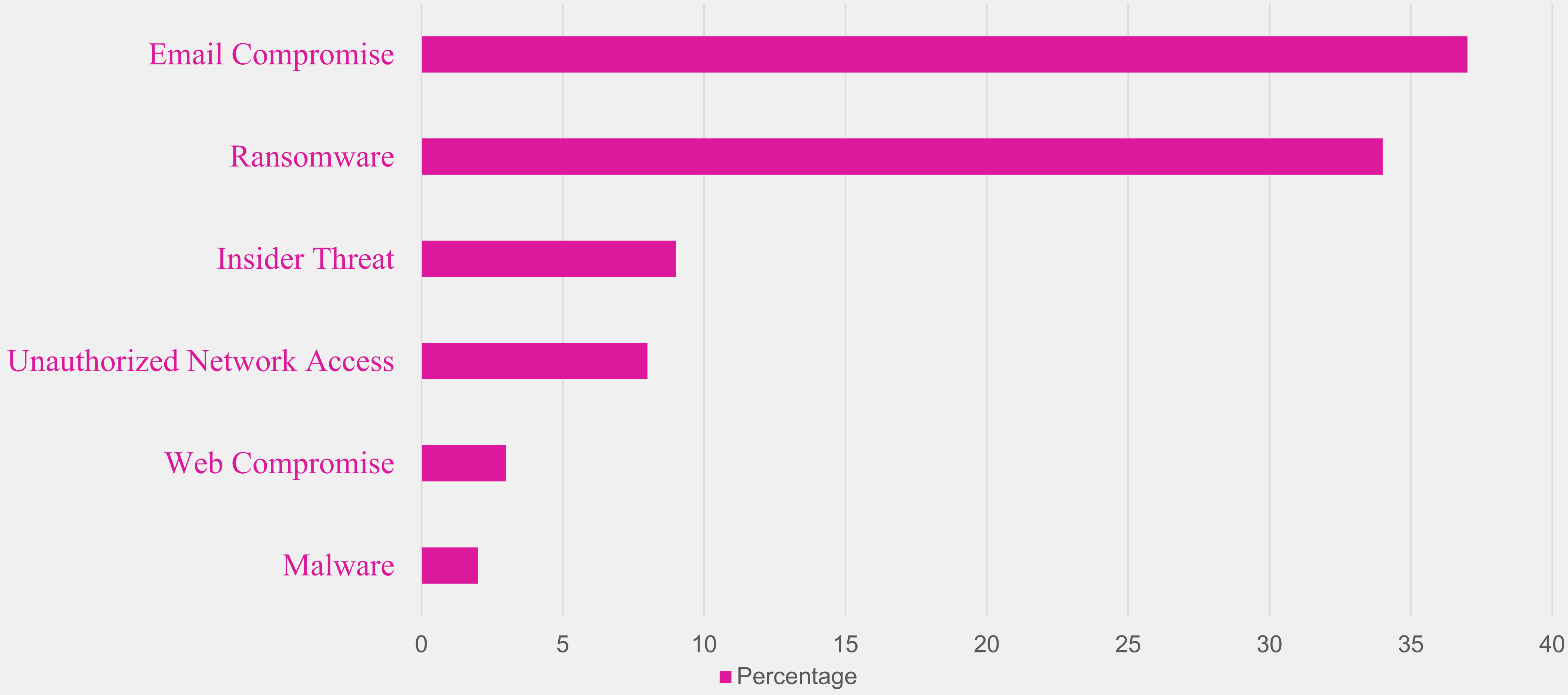
Terms that will be used:

- **Threat actor/bad actor/malicious actor:** Either an individual or group that takes part in an action that is intended to cause harm in the cyber/privacy realm.
- **Data Breach:** The unauthorized exposure, disclosure, or loss of personal information that compromises the security, confidentiality, or integrity of the personal information. (Note: Be mindful not to use prematurely. "Cyber incident" is a better descriptor while a forensic investigation and/or legal analysis in ongoing.)
- **Insured:** The covered entity or active policyholder that has tendered notice of an incident or claim.
- **Cyber Services/Breach Response Services**: Access to and/or the retention of approved incident response vendors from Beazley's curated panel of Service providers.
- **Services Vendor:** A service provider from Beazley's panel of service providers/vendors that assist insureds with cyber and privacy matters.
- **Notification:** Letter sent to a data subject informing them that their data was or was potentially accessed or lost in a breach incident. It must include the type of breach, personal information affected, and advice about what should be done.

Threat Incident Types

- **Email Compromise:** An event where email accounts are accessed maliciously by a third party (e.g., account takeover), a phishing email/campaign is identified, or an organization's email is used or compromised in a fraud scheme, such as a business email compromise (BEC).
- **Ransomware:** An event where threat actors conduct malicious activity within a network followed by a demand for a ransom payment (usually in cryptocurrency). Typically includes some combination of data exfiltration, data encryption, and extortion. Ransom payment would be to obtain a decryption key and/or prevent the release of the impacted data.
- **Malware - Other:** An organization is impacted by malware or virus where no financial demand is made. For example, pre-ransomware activity or the presence of information-stealing malware.
- **Unauthorized Access:** An unauthorized actor has inadvertently or maliciously accessed a network.
- **Insider Threat:** Person within an organization, or a contractor, has access to assets or inside information concerning the organization's security practices, data, and computer systems and uses the information to negatively impact the organization.
- **Web Compromise:** An actor has gained unauthorized access to web application or website code to conduct malicious activity. For example, SQL injections to steal credit card data or website defacement.

Breach Response Services Vendor:
Most Common Threat Incident Type Targeting Healthcare 2023

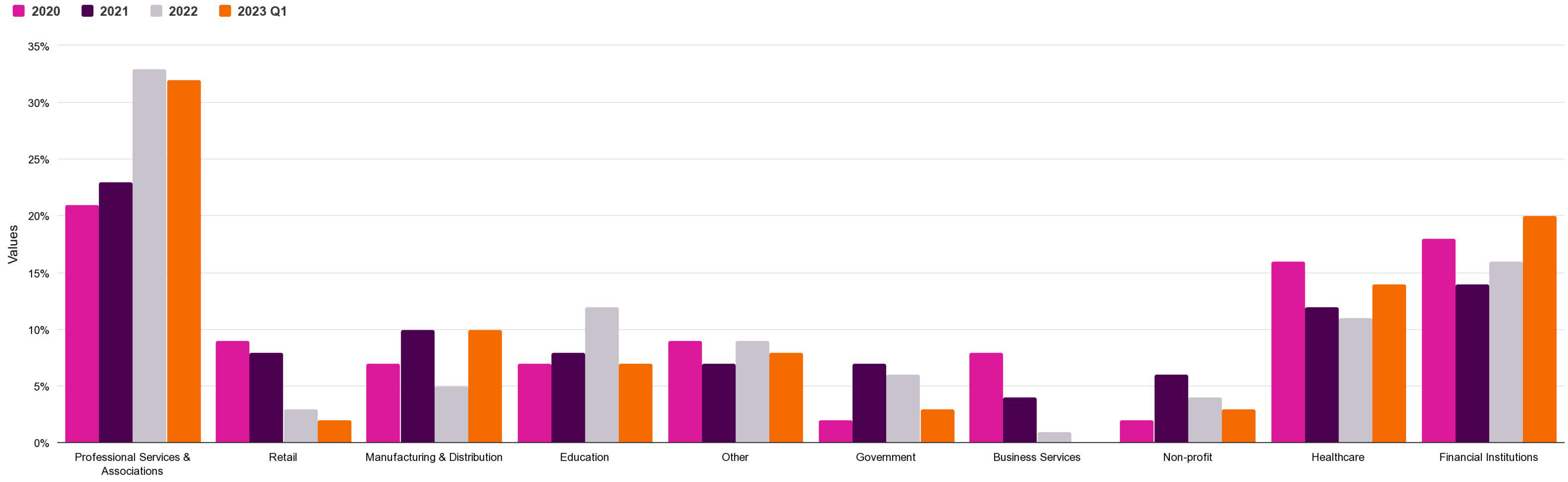


beazley

BEC Prominent Cause of Loss and Rising

Business Email Compromise

Percentages by industry.



Beazley Spotlight On Cyber & Technology Risk 2023

Healthcare Ransomware Statistics Relative to Other Industries 2023

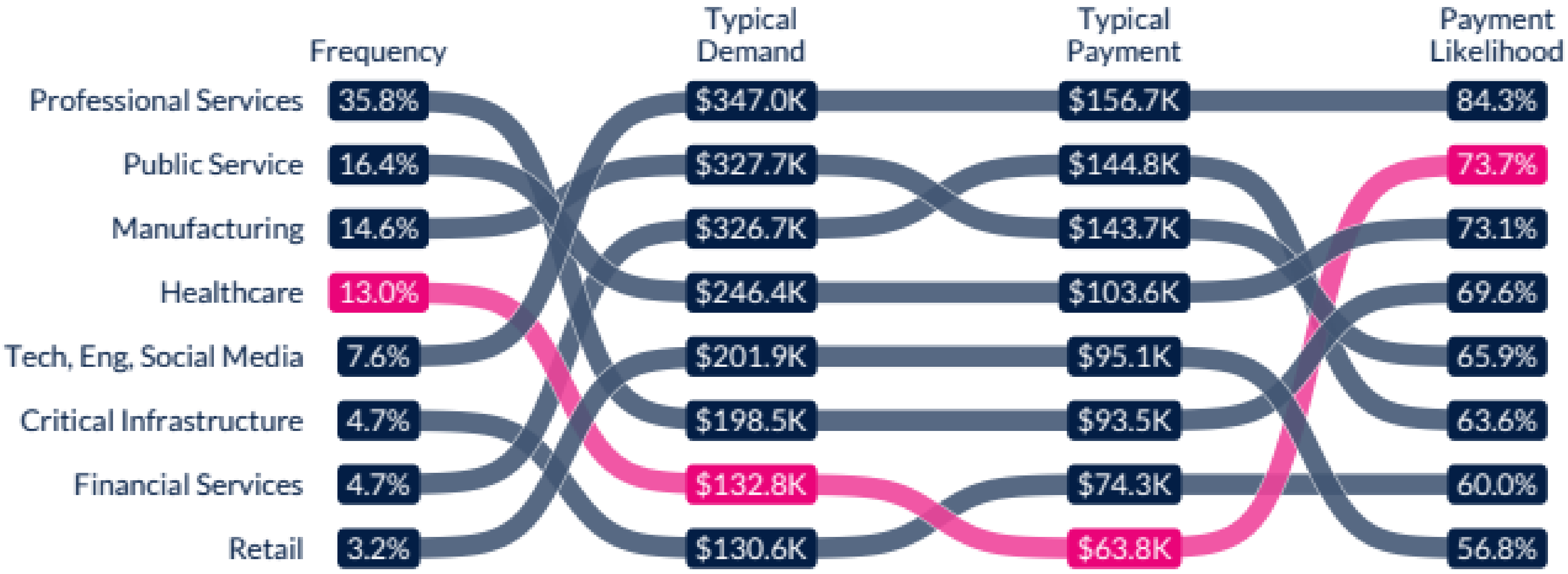


Figure 1—Sector's important values compared to others

Arete Healthcare Sector Report 2023

10 Tips for Cybersecurity in Healthcare

01
Establish a Security Culture

02
Protect Mobile Devices

03
Maintain Good Computer Habits

04
Use a Firewall

05
Install and Maintain Anti-Virus Software

06
Plan for the Unexpected

07
Control Access to Protected Health Information

08
Use Strong Passwords and Change Them Regularly

09
Limit Network Access

10
Control Physical Access

www.healthit.gov

1. Establish a Security Culture

- The weakest link in any computer system is the user. One of the most challenging aspects of instilling a security focus among users is overcoming the perception that “it can’t happen to me.” People, regardless of their level of education or IT sophistication, are alike in believing that they “will never succumb to sloppy practices or place patient information at risk. That only happens to other people.” A security-minded organizational culture is paramount to safeguarding against threat actors.
- Security practices must be built in, not bolted on. No checklist can adequately describe all that must be done to establish an organization's security culture, but there are some obvious steps that must be taken:
  - Education and training must be frequent and ongoing.
  - Those who manage and direct the work of others must set a good example and resist the temptation to indulge in exceptionalism.
  - Accountability and taking responsibility for information security must be among the organization’s core values.
- Protecting patients through good information security practices should be as second nature to healthcare organizations as sanitary practices. Measures to reduce risk are only effective if the healthcare entity is willing and able to implement them, to enforce policies that require the appropriate safeguards to be used, and to effectively and proactively train all users so that they are sensitized to the importance of information security.

2. Protect Mobile Devices

- Mobile devices—laptop computers, handhelds, smartphones, portable storage media—have opened a world of opportunities to untether Electronic Health Records from the desktop, but this also presents threats to information privacy and security.
- Because of their mobility, these devices are easy to lose and vulnerable to theft.
- Mobile devices are more likely than stationary ones to be exposed to electromagnetic interference and corruption of the information stored on them.
- Mobile devices may be used in places where the device can be seen by others, so extra care must be taken by the user to prevent unauthorized viewing of the electronic health information displayed on a laptop or handheld device.
- Not all mobile devices are equipped with strong authentication and access controls. Extra steps may be necessary to secure mobile devices from unauthorized use. Laptops should have password protection similar to the examples in Tip 8. Many handheld devices can be configured with password protection, and these protections should be enabled when available. If password protection is not provided, additional steps must be taken to protect electronic health information on the handheld, including extra precaution over the physical control of the device.
- Laptop computers and handheld devices are often used to transmit and receive data wirelessly. These wireless communications must be protected from eavesdropping and interception (Tip 9 describes wireless network protection). Cybersecurity experts recommend not transmitting electronic health information across public networks without encryption.

3. Maintain Good Computer Habits

- IT systems, including EHR systems, must be properly maintained so that they can continue to function properly and reliably in a manner that respects the importance and the sensitive nature of the information stored within them.
- **Configuration Management**
  - Uninstall any software that is not essential to running the practice (e.g., games, instant messaging applications, photo-sharing tools).
  - If the purpose of the software application is not obvious, do some research to learn more about its uses. When in doubt, check with an EHR developer to see if a particular software is critical to its function.
  - Do not simply accept defaults or standard configurations when installing software. Go through each option and understand the choices presented; get technical assistance where necessary
  - Find out about any "back doors" or open connections between the vendor and the software. If there are any, ensure there's a secure connection at the firewall and request that it be disabled when not in use.
  - Disable remote file sharing and remote printing within the operating system configuration. Having these enabled could result in accidental sharing or printing of files to unintended locations where unauthorized individuals could access them.
- **Software Maintenance**
  - Most software requires periodic updating to keep it secure and to add features. Vendors may send out updates in various ways, including automated downloads and downloads by request.
  - Updates can address newly found vulnerabilities in the product. In larger enterprises, there can be daily "patching" as multiple vendors may issue frequent updates. In smaller practices, there may not be resources to continually monitor for and implement updates.

3. Maintain Good Computer Habits (cont.)

  - Where resources are limited, still the onus is on the practice to monitor for critical and urgent patches that require immediate action. Attention needs to be given to messages from vendors with patches and updates that should be acted upon as soon as possible.

- **Operating System (OS) Maintenance**
  - Over time, an OS tends to accumulate outdated information and settings unless regular maintenance is performed. Similar to how a healthcare entity makes sure that medical supplies have not expired, materials that are out-of-date on a computer system must be dealt with.
  - Disable user accounts for former employees in a timely fashion. In cases where an employee is terminated, disable the access to the account prior to the notice of termination being served.
  - Sanitize computers and any other devices, such as copy machines, before they are disposed of. Even if all the data on a hard drive has been deleted, it may be possible to recover it with commonly available tools.
  - Software that is no longer needed should be fully uninstalled (including “trial” software and old versions of the current software).

4. Use a Firewall

- A firewall protects against intrusions and threats from outside sources. Anti-virus software will help to find and destroy malicious software that has already entered, a firewall's position is to prevent intruders from entering in the first place--infection control vs. disease prevention.
- A firewall can take the form of a software product or a hardware device. In either case, its job is to inspect all incoming messages to the system (either from the Internet or a local network) and decide, according to pre-determined criteria, whether the message should be allowed in.
- Configuring hardware firewalls can be technically complicated and should be done by trained technical personnel. Software firewalls, are often pre-configured with common settings that then to be useful in many situations. Software firewalls are included with some popular operating systems, providing protection at the installation stage. Anti-virus suppliers and security vendors can have firewall software that come with technical support and configuration guidance that users with limited technical expertise can take advantage of.
- Large practices that use a Local Area Network (LAN) should consider hardware firewall. The hardware firewall sits between the LAN and the internet, providing centralized management of firewall settings. This increases security of the LAN, as it ensures that the firewall settings are uniform for all users. Hardware firewall will likely need to be monitored and maintained by a specialist.

5. Install and Maintain Anti-Virus Software

- Without anti-virus software, data may be stolen or destroyed, and threat actors could take control of a machine. Compromises happen through viruses and similar code that exploits vulnerabilities.
- It is important to keep anti-virus software up-to-date. Anti-virus products require regular updates from the vendor in order to protect against the newest computer viruses and malware. Most will automatically generate update reminders and are configurable to allow for automated updating.
- Even a system that has all the latest security updates could still be susceptible to compromise because of previously undetected flaws. Thumb drives, malicious emails and web downloads could be used by bad actors to do harm, so need to have the most robust AV detection capabilities.
- Typical Symptoms of an infected computer:
  - System will not start normally (e.g., blue screen)
  - System repeatedly crashes for no obvious reason
  - Internet browser goes to unwanted web pages
  - Anti-virus software does not appear to be working
  - Many unwanted advertisements pop up on the screen
  - The user cannot control the mouse/pointer

6. Plan for the Unexpected

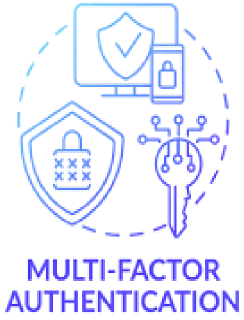
- Important healthcare records and other vital assets need to be protected against loss from a variety of events—natural disasters, cyber incidents and other mad-made incidents.
- Two key parts to protection: creating backups and having a sound recovery plan.
- From the first day a new HER is functioning in a practice, the information must be backed up regularly and reliably. Reliability means that it can be counted on in an emergency—data correctly captured and can quickly and accurately be restored.
- Important to test regularly to ensure that the backup media is able to restore properly. To the extent possible, an automated backup method should be used.
- Backups are only as good as their ability to be protected from the same event that befalls the main system. Protection could mean physical storage at another secure location or the use of carefully selected, secure cloud backup options.
- Important to maintain the same level of access controls for the backups as the main systems.
- Recovery planning is essential--clear procedures in place in the event of a cyber attack or other emergency. Preparation for a possible scenario where an entity is called upon to rapidly supply medical records and information.
- Knowledge of where the data is backed up, when they were done (timeframe and frequency), where backups are stored, type of equipment needed for restoration, who is responsible to lead restoration effort.

7. Control Access to Protected Health Information

- A password is only half of what makes up a computer user's credentials. The other half is the user's identity, or username.
- Username and password combinations are used as part of an access control system in which users are assigned certain rights to access the data. This access control system might be part of an operating system (e.g., Windows) or built into a particular application (e.g., an e-prescribing module).
- Configure EHR implementation to grant electronic health information access only to people with a “need to know.” File access permissions can be set using an access control list. Someone with the proper authorizations and access needs to identify which files should be accessible to which staff members in particular.
- Role-based access configurations—a staff member’s role within a practice (e.g., physician, nurse, billing specialist) determines what information may be accessed. It is essential to assign staff to the correct roles and then to set the access permissions for each role correctly with respect to the need to know. The combination of regulations and the varieties of access control possibilities make this one of the more complex processes involved in setting up an EHR system in a small practice.
- In certain circumstances, electronic health information that is accessed without permission will be considered a breach that has to be reported to HHS and/or a state agency depending on jurisdiction. Having good access controls and the ability to review access logs to see who has viewed or used information can help with prevention or detection of such data breaches.

8. Use Strong Passwords and Change Them Regularly

- What is the first line of defense in preventing unauthorized access to any computer? Passwords!
- Strong passwords are very important. The strength of the password relates to how hard it is to guess. Since attackers may use automated methods to try to guess a password, it is important to choose a password that does not have characteristics that could make it vulnerable.
- Although a strong password will not prevent threat actors from trying to gain access, it can slow them down and discourage them from carrying out their intended mission.
- Combined with effective access controls, strong passwords can help to prevent casual misuse, such as curious staff members trying to access information they have no legitimate reason to access.
- Systems should be configured so that passwords must be changed on a regular basis. It reduces some of the risk that a system will be easily broken into with a stolen password.
- Strong Passwords should not include:
  - Dictionary words, even if they are slightly altered (e.g., replacing a letter with a number)
  - Personal information such as birth date; names of self, family members, or pets; social security number; or anything else that could easily be learned by others. Remember: If a piece of information is on a social networking site, it should never be used in a password.
- Strong password characteristics:
  - At least eight characters in length (the longer the better)
  - A combination of upper case and lower case letters, one number, and at least one special character, such as a punctuation mark.
- **Multi Factor Authentication (MFA)** - It combines multiple different authentication methods, resulting in stronger security. Entering a password is one factor, and then there is at least another factor, such as getting a text with a code to enter, using an authentication application, answering a secret question, or scanning a fingerprint.



9. Limit Network Access

- Given the sensitivity of health care information and the fact that it is protected by law, tools that might allow outsiders to gain access to a health care practice's network must be used with extreme caution.
- It is crucial to secure a wireless signal so that only those who are permitted to access the information can pick up the signal. Wireless routers should be operated in encrypted mode.
- Be mindful of the range of wireless signals and the fact that they can be picked up from a good distance if they are unsecured--parking lots, other offices in a building, and even nearby dwellings.
- Devices brought into the practice by visitors to the practice should not be allowed access to the network; such devices cannot be fully vetted for security on short notice.
- When the wireless network is configured, each legitimate device must be identified to the router, and only then can the device be permitted access.
- Be mindful of the fact that peer-to-peer applications like file sharing and instant messaging apps can expose the connected devices to security threats and vulnerabilities, including allowing unauthorized access to the devices on which they are installed.
- Understand any risks when deciding to install software or applications; have appropriate approval protocols in place. Also, there may be exploitable bits of code that are not removed even when software or an application gets deleted.

10. Control Physical Access

- Keep devices that make up an EHR system safe from unauthorized access.
- Loss or theft of devices is one of the leading ways that electronic health information is compromised; it is important to limit the chances for a device to be lost, stolen, and susceptible to tampering.
- Data storage devices include portable storage media (thumb or flash drives), laptops, handhelds, desktop computers, hard drives ripped out of machines, lost and stolen backup tapes, and entire network servers.
- Have policies that limit physical access to devices and information. For example, locking machines in rooms with restricted access, managing access to any physical keys, and restricting the ability to remove devices from secure areas.
- Environmental protections/considerations — A server should be kept safe from fire, water, and other elements as best as possible. Keep off floors/near windows where there could be a leak; keep in a temperature-regulated environment.

Healthcare Pixel Litigation

Some healthcare entities have embedded Meta and other pixels on their websites, which send data to Facebook and other third parties for targeted advertising.

Healthcare Pixel Litigation

Variety of claims pled:

- invasion of privacy claims
- Wiretapping
- state statutory claims
- breach of contract, negligence, negligent misrepresentation, and unjust enrichment.

High Volume – More than 200 class actions filed over the last year. 2022 was the start of an inflection point. HHS has updated its guidance to be clear about what isn’t allowed.

Hard to Settle

- Mass General in Birmingham - $18.4M settlement in January 2022 set a bar. They used cookies, pixels, website analytics tools, and associated technologies on several websites without first obtaining the consent of website visitors.
- Mixed caselaw
- Plaintiffs counsel that don’t typically work in the data breach/privacy space

CIPA (California Invasion of Privacy Act)

- CIPA is a privacy law that went into effect in 1994 with the aim of protecting residents of California from privacy violations that occur when communications are listened to or recorded without knowledge or consent – Anti wiretapping / anti eavesdropping statute.

- It applies if one party to the communication is a resident of California, meaning a business entity does not need to be located in CA for the law to apply.

- In CA, do not need to show harm, just have the pixels or associated technology installed.

- Core to wiretapping is communication is being read, interpreted or listened to (but not necessarily recorded) in real time.

- Chat Boxes – reading, learning, and responding to users. Chat Box features are often from a third-party, not website operator.

Wiretapping

Impact:

- Anyone using pixels on their website

History:

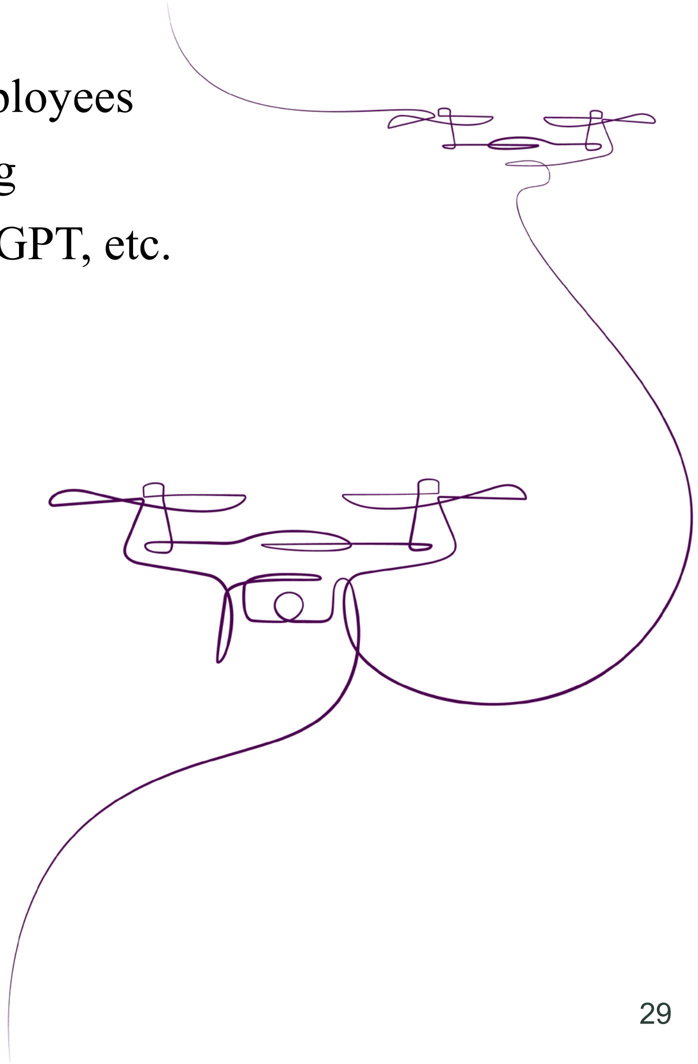
- Early case law mostly favorable
- *Harriet Carter* – August 2022, Third Circuit held use of pixels could be considered an "interception" of a "communication" in violation of PA's wiretapping statute
- Flood of claims – mostly two-party consent states (PA, CA, WA)

Where Are These Heading:

- Settlement:
  - No big public settlements
  - Statutory penalties - $1,000, $2,500 or more per violation
- Mixed decisions: e.g., Noom (sensitive data) vs GameStop (not sensitive)

Future Risks For Healthcare Organizations: What’s Next?

- BECs: Threat actors impersonating employees
- Threat of vishing and social engineering
- AI & deep fakes, including use of ChatGPT, etc.
- Future legal and regulatory activity



Questions?

Thank You.