Cybersecurity in Healthcare

Landscape and Threats

MedPro Group
a Berkshire Hathaway company

Speaker bio

Richard A. Bryan, MSN, RN, CPHRM, Senior Patient Safety & Risk Consultant, MedPro Group (Richard.Bryan@medpro.com)

Richard has more 40 years of experience in healthcare, including military, not-for-profit, and teaching facilities as well as the private sector. He has served in progressive leadership roles in nursing management, risk management, and insurance.

Most recently, Richard held an executive leadership role in a healthcare system with 1 hospital and 28 primary care/multi-specialty clinics. During his tenure, his areas of responsibility included risk management, patient safety, insurance, compliance, regulatory readiness, quality, care management, population health and clinical integration, clinical operations of behavioral health and women's and children's services, Epic implementation, and ongoing Epic operations team and information services.

Richard earned a bachelor of science degree in nursing from Union University and a master of science degree in nursing with a major in healthcare systems management from Loyola University New Orleans.

Richard is a member of the American Society for Health Care Risk Management, the Washington Healthcare Risk Management Society, Oregon Society for Healthcare Risk Management, the American College of Healthcare Executives, and the Medical Group Management Association. He is also a certified professional in healthcare risk management.

Designation of continuing education credit

MedPro Group is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

MedPro Group designates this enduring activity for a maximum of 1.0 *AMA PRA Category 1 Credits*™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

MedPro Group
Nationally Approved PACE Program
Provider for FAGD/MAGD credit.
Approval does not imply acceptance by
any regulatory authority or AGD endorsement.
October 1, 2018 to September 30, 2022
Provider ID# 218784

MedPro Group designates this continuing dental education activity as meeting the criteria for up to 1 hour of continuing education credit. Doctors should claim only those hours actually spent in the activity.

Disclosure

MedPro Group receives no commercial support from any ineligible company/ commercial interest.

It is the policy of MedPro Group to require that all parties in a position to influence the content of this activity disclose the existence of any relevant financial relationship with any ineligible company/commercial interest.

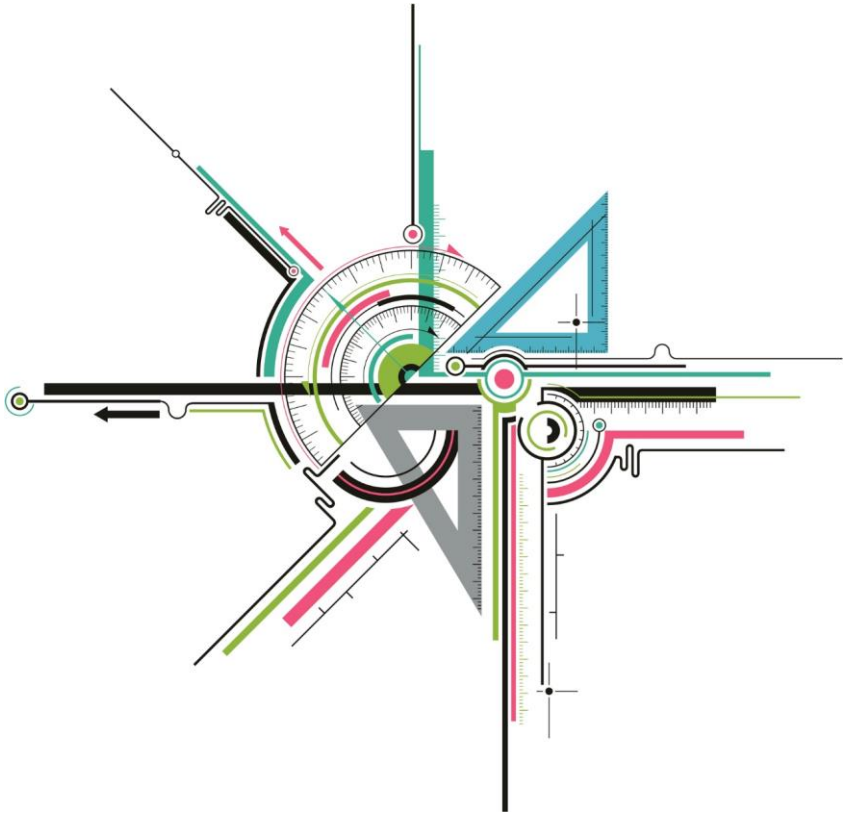
When there are relevant financial relationships mitigation steps are taken. Additionally, the individual(s) will be listed by name, along with the name of the commercial interest with which the person has a relationship and the nature of the relationship.

Today's faculty, as well as CE planners, content developers, reviewers, editors, and Patient Safety & Risk Solutions staff at MedPro Group have reported that they have no relevant financial relationships with any commercial interests.

Objectives

At the conclusion of this program, participants should be able to:

- Possess a better overall understanding of cybersecurity terminology and the impact of cyber risks on practices and/or healthcare facilities
- Understand the costs associated with healthcare breaches and cyber liability claims
- Recognize the most common threats and why cyber attacks are increasing



Glossary of terms

Common terminology

- Anti-virus/Anti-malware software – Programs designed to detect different forms of malware (e.g., viruses and spyware) and prevent them from infecting computers. Some software may also be used to clean already-infected computers.
- Business email scams – Scams designed to target businesses by using social engineering or computer intrusion to compromise legitimate business email accounts and conduct unauthorized fund transfers or obtain personal information.
- Cyber crime – Crime committed on the internet or aided by the use of computer technology.
- Cyber incident/Cyber breach – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable use policies.
- Cyber insurance – Insurance that is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage.
- Cybersecurity – Efforts or processes designed to prevent or manage the risk of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, to strengthen the confidentiality, integrity, and availability of these systems.

A great resource for terminology:
National Institute of Standards and Technology (NIST) Online Glossary https://csrc.nist.gov/glossary

Common terminology (continued)

- Data breach – Incident involving sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit card numbers, personal health information, customer data, company trade secrets, or matters of national security, for example.
- Digital forensics (forensics) – Practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
- Hacker – Individual who attempts to or gains access to an information system, usually in an unauthorized manner. A “white hat” hacker is a cybersecurity specialist who breaks into systems with a goal of evaluating and ultimately improving the security of an organization’s systems.
- Malware – A computer program covertly placed onto a computer or electronic device with the intent to compromise the confidentiality, integrity, or availability of data, applications, or operating systems. Common types of malware include viruses, worms, malicious mobile code, Trojan horses, rootkits, spyware, and some forms of adware.
- Patch – Software code written to repair or “fix” a software program. When a software developer or distributor learns of a security weakness, a patch is the usual immediate solution that is provided to users and can sometimes be downloaded from the software maker’s website.

A great resource for terminology:
National Institute of Standards and Technology (NIST) Online Glossary https://csrc.nist.gov/glossary

Common terminology (continued)

- Viruses – Computer program designed to copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.
- Virtual private network (VPN) – Virtual network built on top of existing networks to provide a secure communications mechanism for data and internet protocol (IP) information transmitted via the virtual network.
- Vulnerability – Weakness in a system, application, or network that allows exploitation or misuse.
- Watering hole attack – Security exploit where the attacker infects websites that are frequently visited by members of the group being attacked, with a goal of infecting a computer used by one of the targeted group when they visit the infected website.
- Whitelist – Approved list or register of entities provided a particular privilege, service, mobility, access, or recognition within a defined computer system (e.g., individual or network).
- Wiping – Overwriting media (like a hard drive) or portions of media to hinder reconstruction of the data.

A great resource for terminology:
National Institute of Standards and Technology (NIST) Online Glossary https://csrc.nist.gov/glossary

The impact

Cyberattacks and ransomware

NEWS

Ransomware attack on Cass Regional shuts down EHR

by **Jessica Davis** | July 11, 2018

Emergency and stroke patients are still being diverted to ensure patients receive the best possible care, but the Missouri health system

Allscripts hit by ransomware, knocking some services offline

by **Jessica Davis** | January 19, 2018

Users took to Twitter to complain about the cloud EHR being down, with some unable to access patient information all day.

Primary Health Care announces email breach one year after discovery

by **Jessica Davis** | March 19, 2018

Hackers broke into four employee email accounts of the Iowa provider, allowing access to a wide range of sensitive data.

NEWS

Phishing attacks breach Alive Hospice for 1 to 4 months

by **Jessica Davis** | July 18, 2018

Two employee email accounts were breached by phishing attacks, which potentially gave hackers access to a trove of highly sensitive

NEWS

Phishing hack on Ohio provider breaches data of 42,000 patients

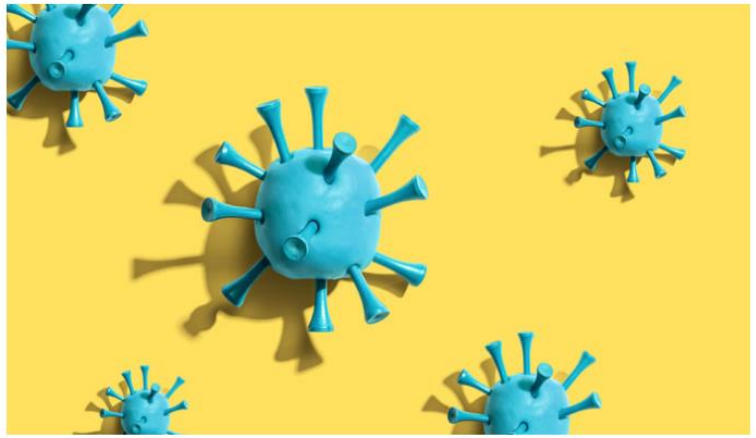
by **Jessica Davis** | May 29, 2018

A hacker hit some email accounts of Aultman Health Foundation with a phishing attack in February, but officials didn't discover the

Cyberattacks and ransomware (continued)

Hackers Hit COVID-19 Biotech Firm, Cold Storage Giant with Cyberattacks

Cold storage giant Americold and Global firm Miltenyi Biotec recently faced cyberattacks; ransomware, an email error, phishing, and an application hack complete this week's breach roundup.



By Jessica Davis

November 18, 2020 - Two global firms with reported ties to the COVID-19 pandemic response faced cyberattacks within the last week. Miltenyi Biotec **reported** a system outage caused by a malware attack, while cold storage giant Americold, previously in talks to provide storage for the distribution of COVID-19 vaccines, experienced a "cybersecurity incident."

COVID-19, Ransomware, Breaches Led 2020 Health IT Security Trends

The COVID-19 outbreak reshaped HHS HIPAA sanctions and enforcement discretion in 2020, which topped health IT security trends, alongside ransomware and data breaches.

By Jessica Davis

January 04, 2021 - In terms of healthcare cybersecurity and overall data breaches, data from 2021 will likely show a year of massive cybercriminal activity and a spike in reported events during the second half of the year. Overall, the leading healthcare cybersecurity trends were

560 Healthcare Providers Fell Victim to Ransomware Attacks in 2020

In 2020, Emsisoft data shows 560 healthcare provider facilities fell victim to ransomware attacks, of an overall 2,354 US entities hit by the malware variant.

By Jessica Davis

January 19, 2021 - In the midst of responding to COVID-19, the healthcare sector faced a significant number of ransomware attacks in 2020 with 560 healthcare provider facilities falling victim to the malware variant, according to the latest Emsisoft State of Ransomware **report**.

What is a health record worth?

Securing patients' electronic protected health information (ePHI) continues to be a top priority for healthcare organizations of all sizes.

The need for vigilance in data security is emphasized by reports suggesting that a complete health record can fetch as much as $1,000 on the dark net.

Keckley, P. (2017, June 9). Is your hospital prime for ransomware attack? *Hospitals & Health Networks Magazine*. Retrieved from www.hhnmag.com/articles/8360-is-your-hospital-prime-for-ransomware-attack;
Socas, J. (2015, December). Growing pains: Cybercrime plagues the healthcare industry. *Healthcare IT News*. Retrieved from www.healthcareitnews.com/blog/growing-pains-cybercrime-plagues-healthcare-industry

The impact is widespread

Wood Ranch Medical, a Simi Valley, California-based medical clinic, lost all access to its patients' electronic health records due to a ransomware attack in August 2019. Due to the extent of the damage to both primary and back-up systems, the clinic closed in December 2019.

Campbell County Health in Wyoming experienced a cyberattack in September 2019 at which time ransomware was introduced into its IT systems. This resulted in the need to transfer patients and reduce services to rebuild the system.

American Dental Association announced a ransomware attack that impacted DDS Safe, a data backup system offered by The Digital Dental Record and PerCSoft Consulting, LLC, which in turn affected hundreds of dental practices.

Janofsky, A. (2019, October 6). Smaller medical providers get burned by ransomware. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/smaller-medical-providers-get-burned-by-ransomware-11570366801?shareToken=sta016f1fa35e646c8ab7f5a74d9b9cead1570366801; Versaci, M. B. (2019, August 30). Ransomware, phishing attacks target dentists. *ADA News*. Retrieved from https://www.ada.org/en/publications/ada-news/2019-archive/august/amid-ransomware-phishing-attacks-dentists-should-take-steps-to-protect-practices.

Increasing number of ransomware attacks

CNN noted that in the 10 months before its report dated October 8, 2019, 140 local governments, police stations, and hospitals had been held hostage by ransomware attacks.

One of the healthcare organizations affected was DCH Health System in western Alabama. DCH, which has three hospitals, had to suspend patient admissions. Unlike many other facilities and organizations, DCH elected to pay the ransom.

In Washington state, Grays Harbor Community Hospital (now called Harbor Regional Health) was hit by ransomware with a demand of payment with bitcoin at a value of $1 million in 2019. FBI advised not to pay, so Grays refused. Later it reached a $185,000 settlement of a class action lawsuit brought on behalf of patients whose PHI has been accessed as a result of the breach.

Kim. A. (2019, October 8). In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks. CNN. Retrieved from https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html; Taylor, S. (2019, October 6). DCH pays hackers responsible for ransomware attack. *Tuscaloosa News*. Retrieved from https://www.tuscaloosanews.com/news/20191005/dch-pays-hackers-responsible-for-ransomware-attack; Sussman, B. (2019, August 19). Hackers demand $1 million after hospital ransomware attack. Secure World Expo. Retrieved from https://www.secureworldexpo.com/industry-news/hospital-ransomware-attack-2019.

Small hospitals, health centers, and physician practices

- Hackers favor small hospitals, health centers, and physician practices
- Smaller providers are prime targets due to the probability that they will pay ransom demand to prevent care disruption
- Research by Risk IQ found that cybercriminals tend to target direct patient care facilities
- National average ransom demand for the 127 analyzed attacks was $59,000

RiskIQ. (2020, April 9). Ransomware in health sector 2020: A perfect storm of new targets and methods. Retrieved from https://www.riskiq.com/wp-content/uploads/2020/04/Ransomware-in-Health-Sector-Intelligence-Brief-RiskIQ.pdf

Cyber liability claims

Healthcare sector (2014-2016)

- Many of the claims occurred in small or mid-sized healthcare organizations
- The average number of records exposed in a healthcare breach was 6 million
- The average breach cost in healthcare was $555,000
- Breaches that exposed protected health information (PHI) were substantially smaller than breaches that exposed personally identifiable information (PII)
- Total average breach cost: PHI – $475,000, PII – $1.85 million
- 63% of healthcare breaches were caused by criminal or malicious activity
- Hacking was the most common cause of loss (20% of cases), with an average cost of $2.4 million

Netdiligence. (2018). 2017 cyber claims study: 2018 spotlight on healthcare. Retrieved from https://netdiligence.com/2018/04/05/netdiligence-releases-analysis-on-healthcare-cyber-claims/

Not all cyber threats involve ransomware

Becker's Hospital Review frequently publishes cybersecurity incidents by month. September and October are the last two months reported with 13 incidents in September and 18 in October.

October 2019:

- Women's Care Florida: 528,188 patients personal and/or health information exposed
- People's Health Centers, St. Louis: 152,000 patients may have had their information viewed
- Kalispell Regional Healthcare: 130,000 patient records may have been exposed
- Methodist Hospitals, Gary, IN: 68,039 patients' protected health information (PHI) may have been exposed
- Prisma Health – Midlands Hospitals, SC: 19,000 patients and 3,000 visitors may have been exposed
- University of Alabama Birmingham Medicine: 19,557 patients may have been exposed
- South Texas Dermatopathology: 15,982 patients may have been exposed

Becker's Hospital Review. (2019, November 1). 18 cybersecurity incidents in October. Retrieved from https://www.beckershospitalreview.com/cybersecurity/18-cybersecurity-incidents-in-october.html

Malware, ransomware, and phishing incidents

Becker's Hospital Review frequently publishes cybersecurity incidents by month.

December 2020

- AspenPointe (now known as Diversus Health) in Colorado Springs notified 295,617 patients of a data breach.
- Hackers based in North Korea launched cyberattacks on drugmakers developing COVID-19 vaccines and treatments.
- The European Medicines Agency was hit by a cyberattack.
- IBM's threat intelligence task force identified a global phishing campaign targeting the COVID-19 vaccine supply chain.
- Greater Baltimore Medical Center HealthCare detected ransomware and shut down many of its IT systems as a result.
- Augusta, Georgia-based University Hospital reported 550 daily cyberattack attempts on its Epic MyChart system.

Becker's Hospital Review. (2020, December 30). 11 healthcare malware, ransomware and phishing incidents in December. Retrieved from https://www.beckershospitalreview.com/cybersecurity/11-healthcare-malware-ransomware-and-phishing-incidents-in-december.html

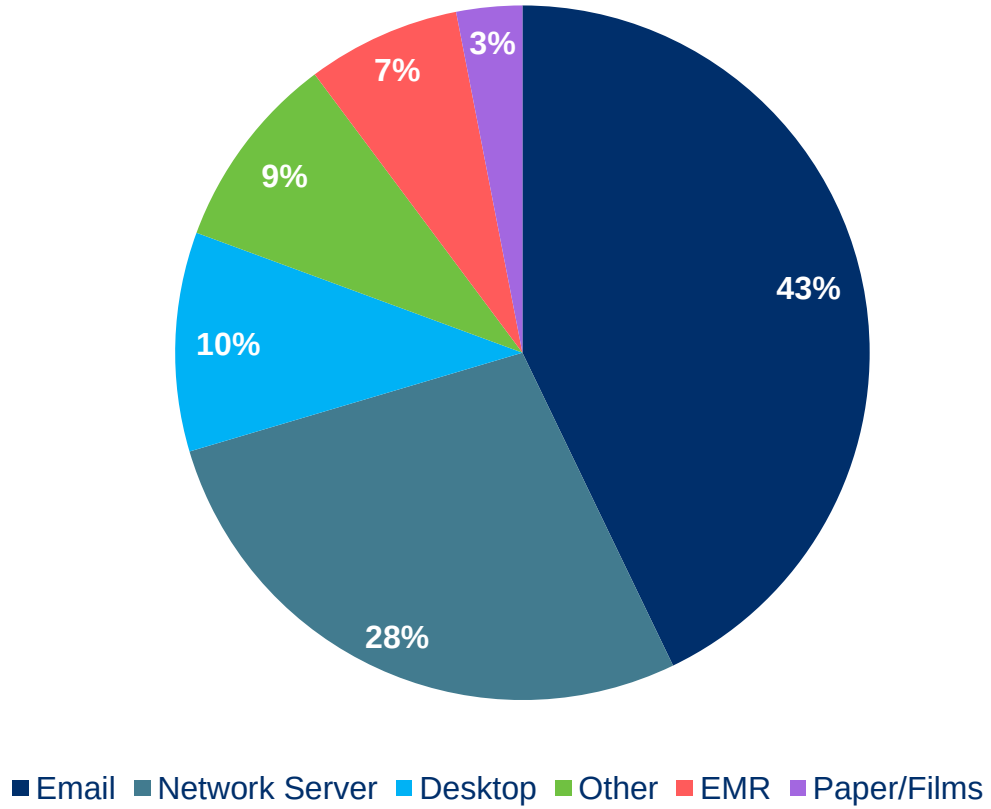
What happens when HHS/OCR receives a breach report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
- Public can search and sort posted breaches
- Receives more than 350 breach reports affecting 500 individuals or more per year
- Opens investigations into a number of smaller breaches as well as breaches affecting 500+ individuals
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (breach notification) and prevent future incidents
  - Entity's compliance before breach

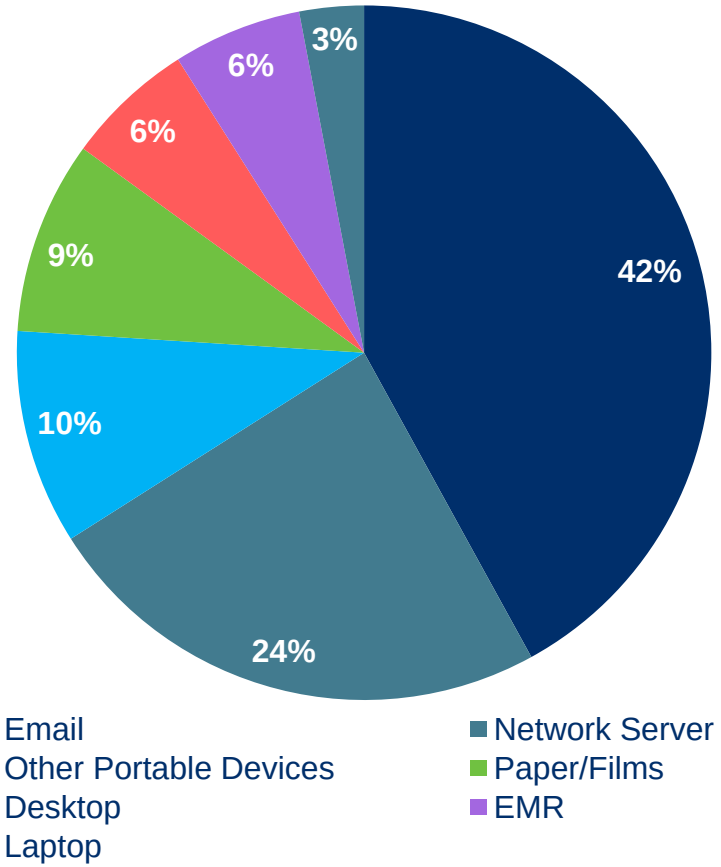
HHS: Department of Health and Human Services
OCR: Office for Civil Rights

500+ breaches by location of breach

May 3, 2018 – April 26, 2019

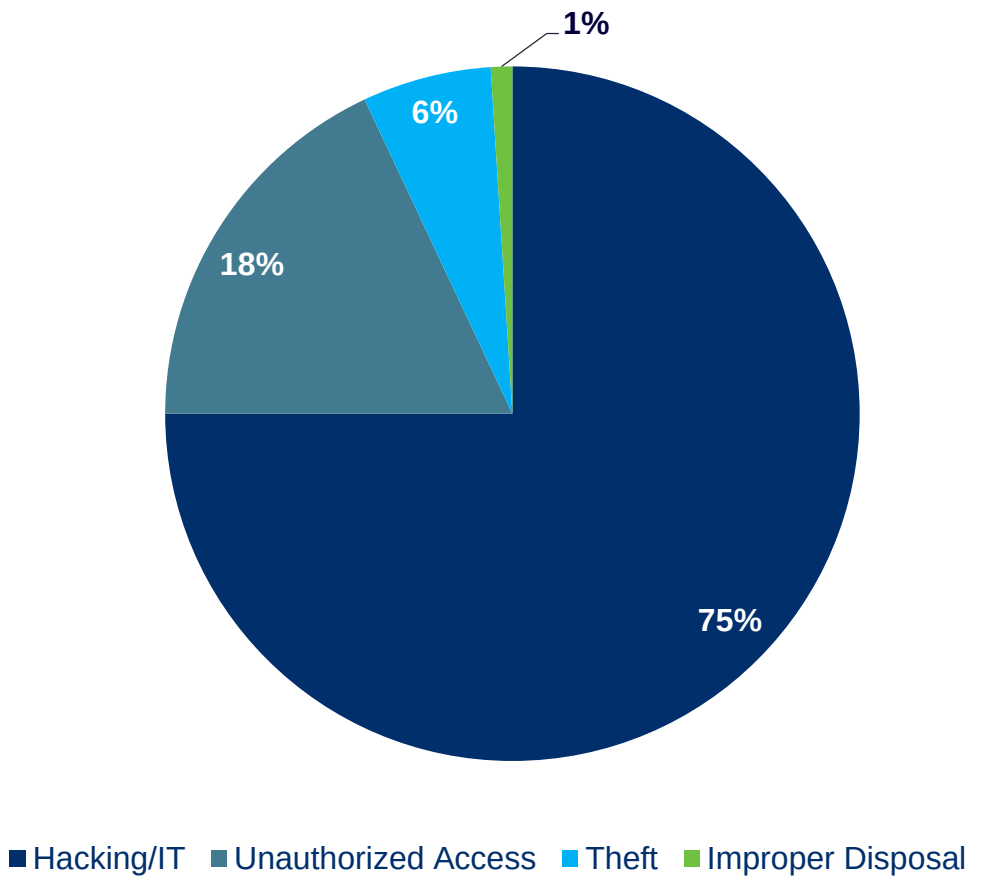


April 29, 2019 – April 27, 2020

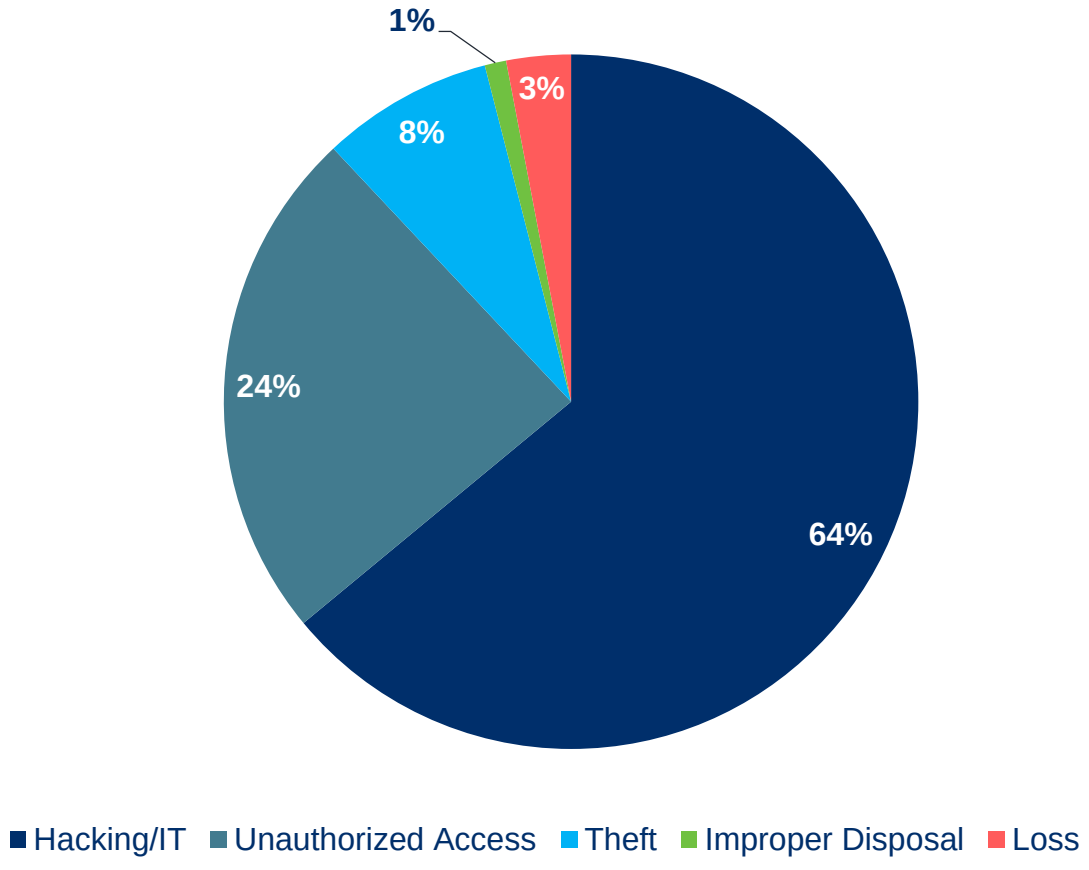


500+ breaches by type of breach

May 3, 2018 – April 26, 2019



April 29, 2019 – April 27, 2020

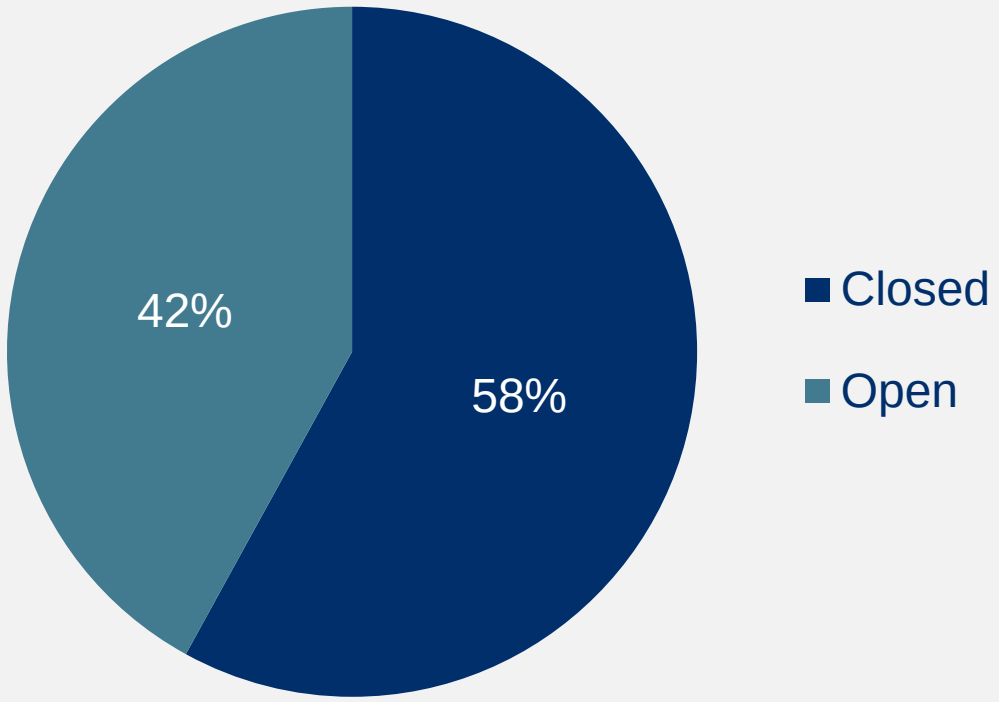


Cyber claims

MedPro Group cyber claims data

Closed claims

- Total dollars paid*
  - > $2,900,000
- Percentage of closed claims with total paid > $1,000
  - 39%
- Average total paid**
  - > $28,000
- Highest total paid claim to date
  - > $118,000K
  - Involved ransomware attack



The number of claims opened in 2019 jumped by 82% over 2018.

Cyber claims: scenarios

Claims	Cost
A former employee recorded a video of a patient and posted it on social media.	> $75,000
An employee accessed a patient's PHI without authorization.	> $47,000
A patient accessed provider's website and clicked on the "contact me" page. After typing & submitting a message, the patient was able to click on another hyperlink that listed 19 names (13 patients and 6 nonpatients) that showed demographics, account numbers, and messages regarding billing.	> $40,000
A ransomware virus infected the insured's computer and deleted all data.	$7,000
A nurse accessed a health record of a friend without consent, unbeknownst to the nurse's employer. The friend sued the physician practice where the nurse worked for a breach of privacy.	$50,000
A computer was stolen from a reception desk area containing the health records of approximately 6,000 patients.	$73,500
An insured inadvertently left its public portal open, resulting in the private data of 10,000 patients being exposed.	$25,000

Cyber claims: additional scenarios

Phishing attack/unauthorized access to emails

Healthcare vendor experienced a breach involving multiple patients

Patient alleges a HIPAA breach when a surgeon allowed an unauthorized person to view the surgery

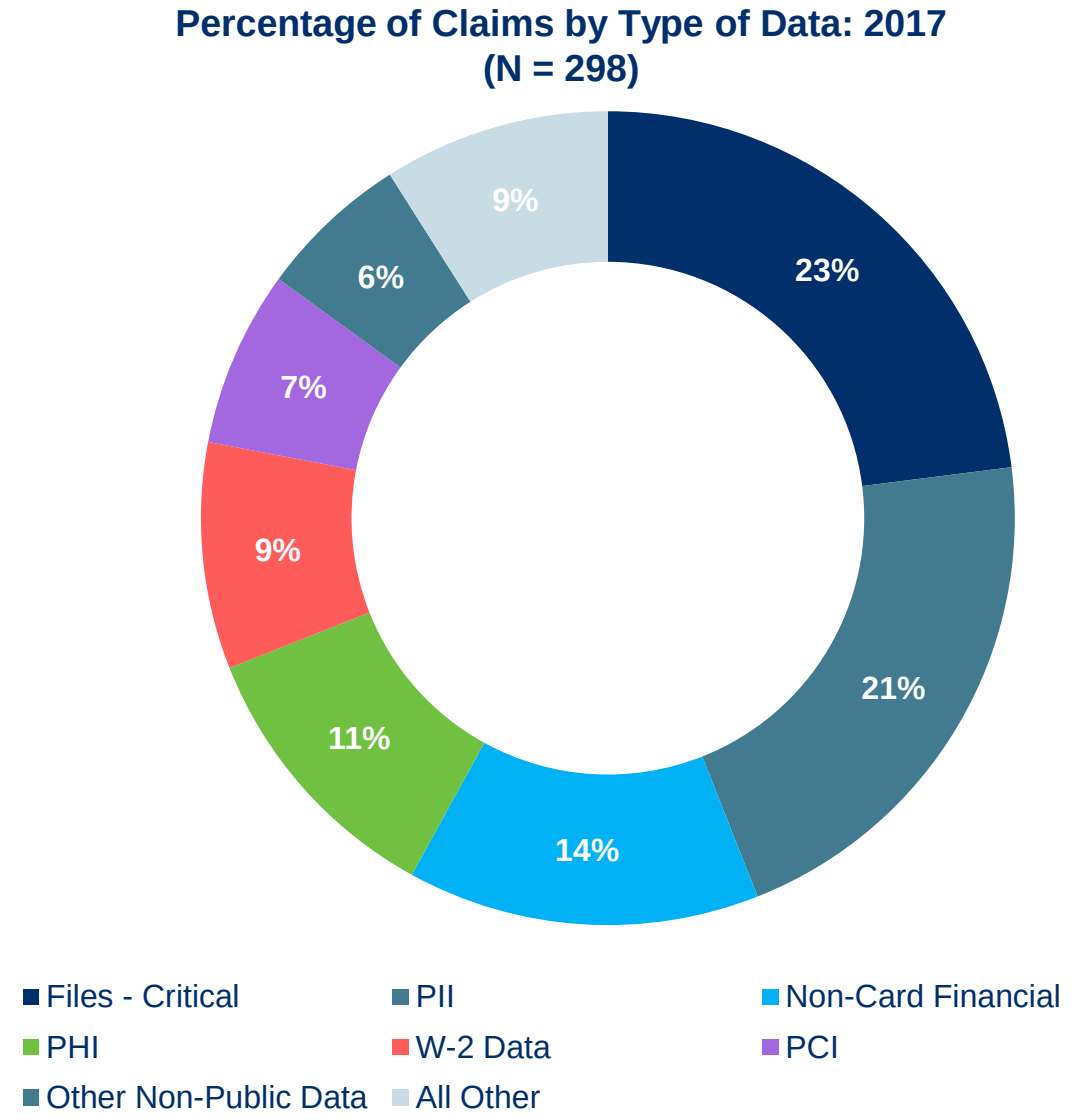
Patients' billing data stolen from a storage unit

Provider sent an email to all patients with exposed email addresses

Multiple patient files stolen from an employee's vehicle

Healthcare industry cyber claims data

- Out of 18 sectors, healthcare ranked 8th in average breach cost when ranked by average.
- Average healthcare breach cost was $555,000; median cost was $68,000.
- Healthcare claims accounted for 17% of claims and 15% of the total breach cost in 2018, versus 15% of claims and 7% of breach costs in 2017.
- Events involving exposure of personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) data accounted for 54% of exposed records claims across all sectors.

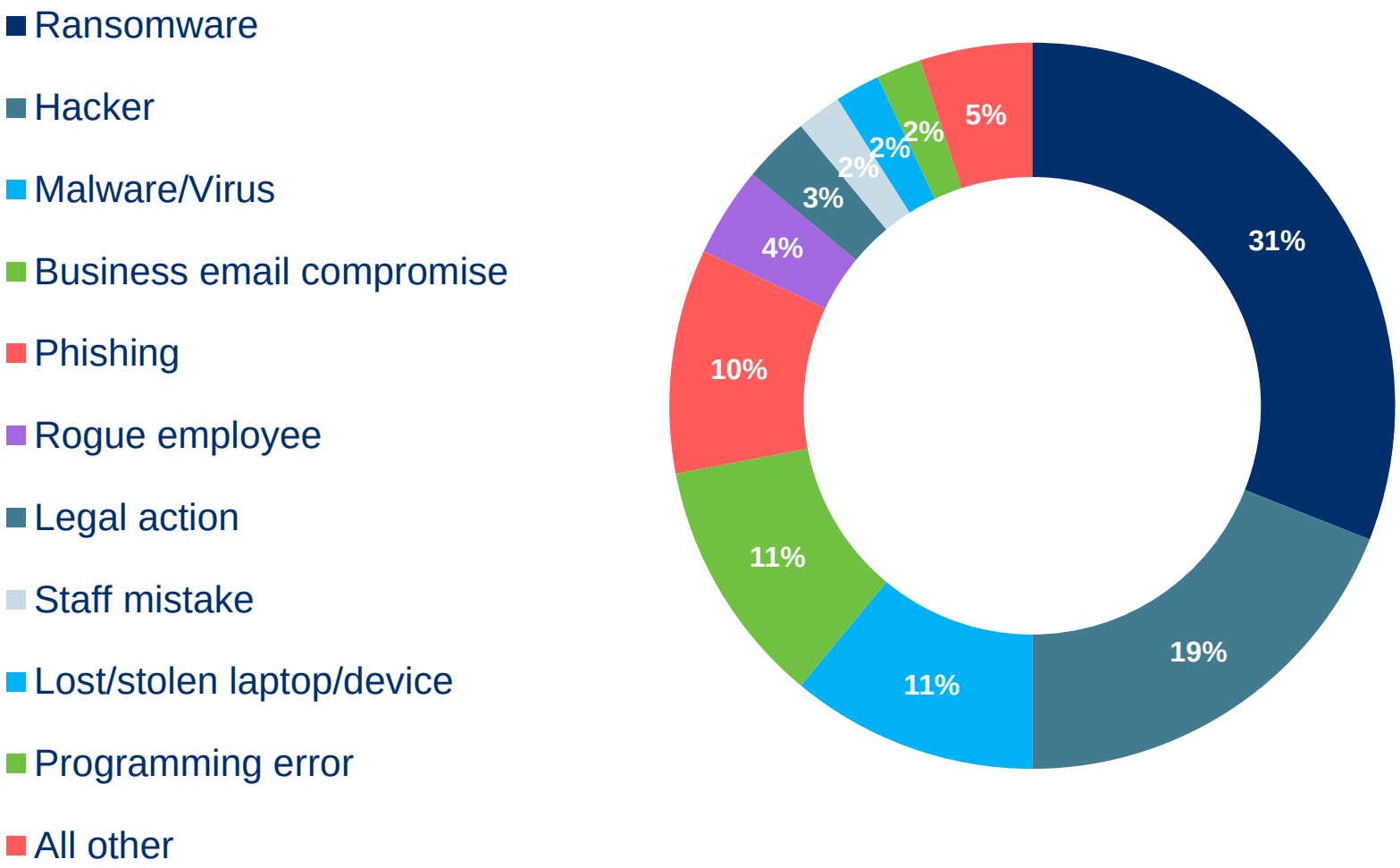


Cyber claims data

The average crisis services cost for the healthcare sector during the 2013 – 2017 period was:	
Forensics	$ 107,000
Notification	$ 581,000
Credit/ID monitoring	$ 203,000
Legal guidance	$ 46,000
Other	$ 100,000
Total	$ 442,000

The total breach cost for the healthcare sector during the 2013 – 2017 period for 199 cases was:	
Average	$ 555,000
Median	$ 68,000
Maximum	$ 15,000,000
Total	$110,448,000

Cyber claims data



Ransomware: average costs by sector

Top 5 by volume of claims based on data from 2015-2019

	Claims	Ransom amount	Crisis services	Total incident cost
Healthcare	312	$26,000	$35,000	$107,000
Professional services	200	$43,000	$50,000	$88,000
Manufacturing	65	$305,000	$47,000	$490,000
Retail	50	$82,000	$48,000	$130,000
Nonprofit	42	$82,000	$105,000	$105,000

Cyber attacks

Defining the threat

Defining the threat

Omaha-World Herald. (2019, August 17). NU faces 'very real' cyber threat: 9.94 million attacks blocked daily. Retrieved from https://omaha.com/news/education/nu-faces-real-cyber-threat-million-attacks-blocked-daily/article_6ef92e13-bb12-5694-856e-7757323a9539.html

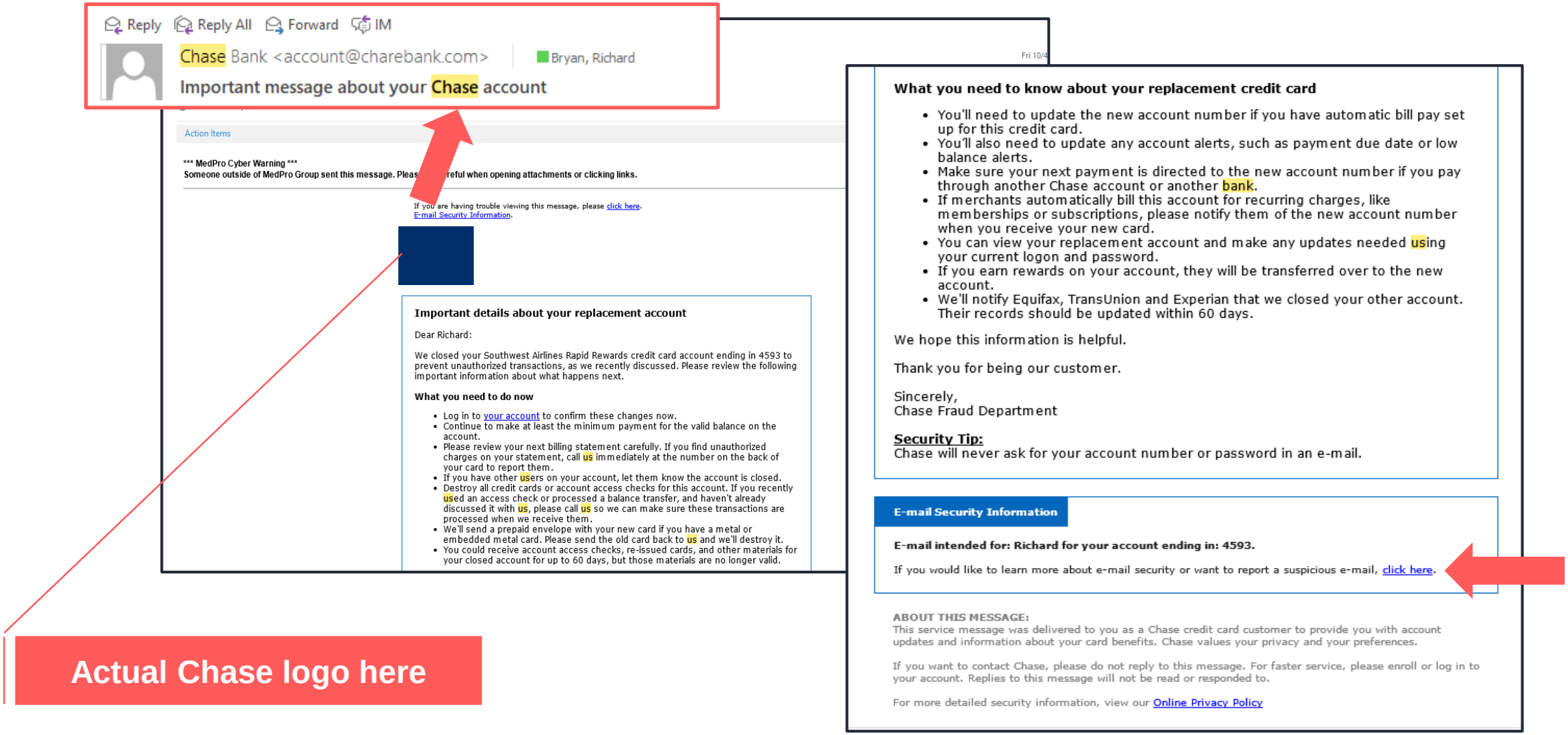
Defining the threat landscape

Social engineering	• Taking actions to influence or manipulate you to prompt you to take some action that facilitates entry into your system.
Phishing	• A form of social engineering whereby a hacker will send out emails to broad groups in an effort to get at least one person to act.
Spear phishing	• The hacker researches an organization then sends personalized emails to targeted individuals to trick the organization into acting in a manner that benefits the hacker.
CEO fraud	• Phishers use an email address similar to that of an authority figure directing the recipient to provide payment or data to particular address.
Pharming	• Hackers hijack a website's domain name and use it to redirect visitors to an imposter site.

Defining the threat landscape (continued)

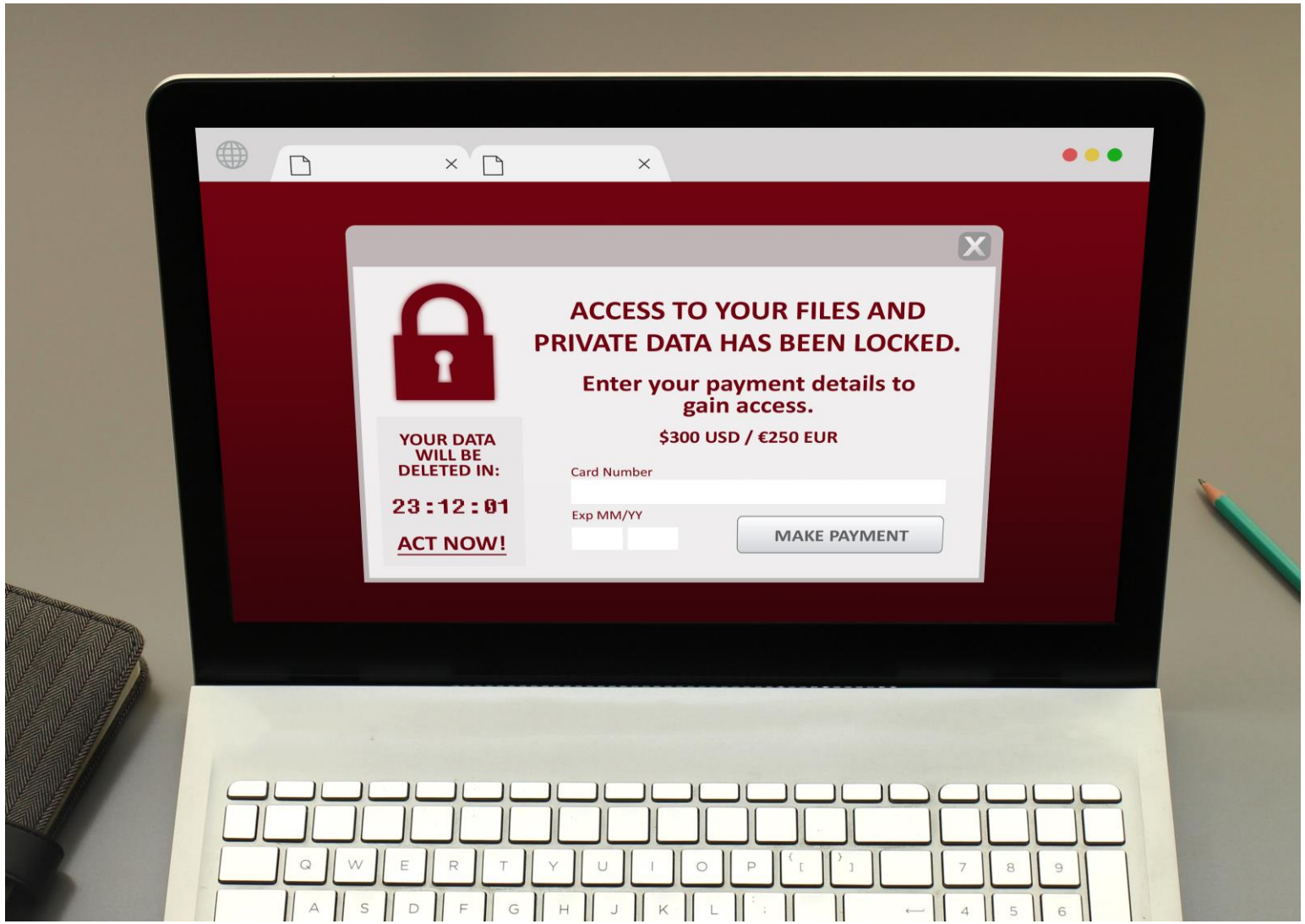
- Island hopping – cyber criminals infiltrate smaller companies proving services to their target organizations
- Three categories of island hopping:
  - Network based island hopping – most common method in which the hacker leverages a victim's network to hop onto an affiliate network.
  - Watering holes – hackers insert malware onto a smaller target website frequently accessed by employees of the larger organization. This in turn infects those visiting the website by providing a gateway to hack the larger organization.
  - Reverse business email compromise (BEC) – hackers take over the email server of the victim company and then use the company's email to send malware attacks to the target company.

Phishing example



Actual Chase logo here

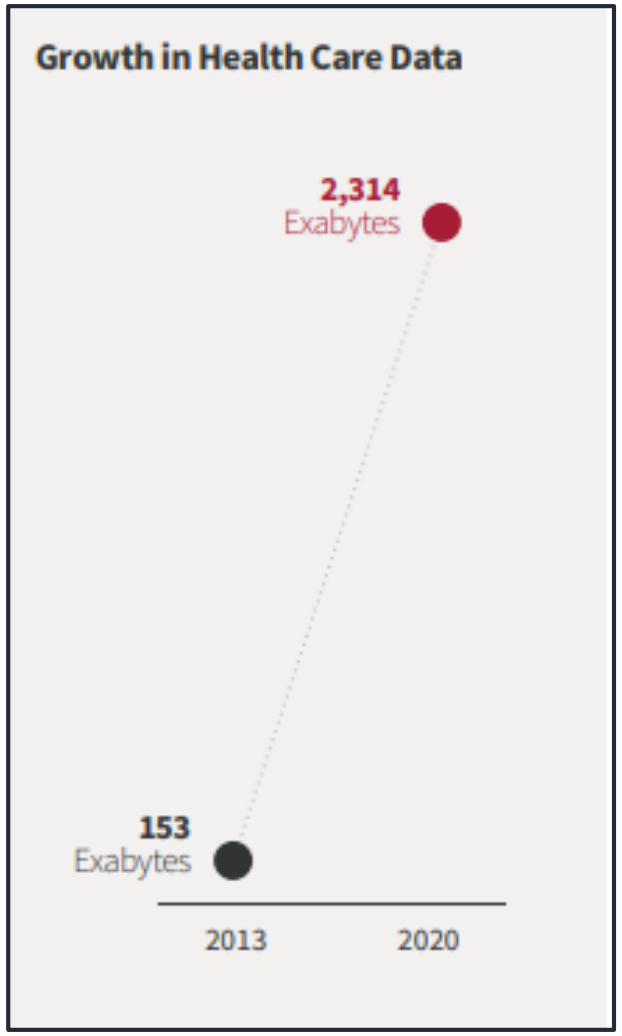
Ransomware notices



Defining the environment

Why are cyber security events increasing?

The explosion of technology and dependence on data

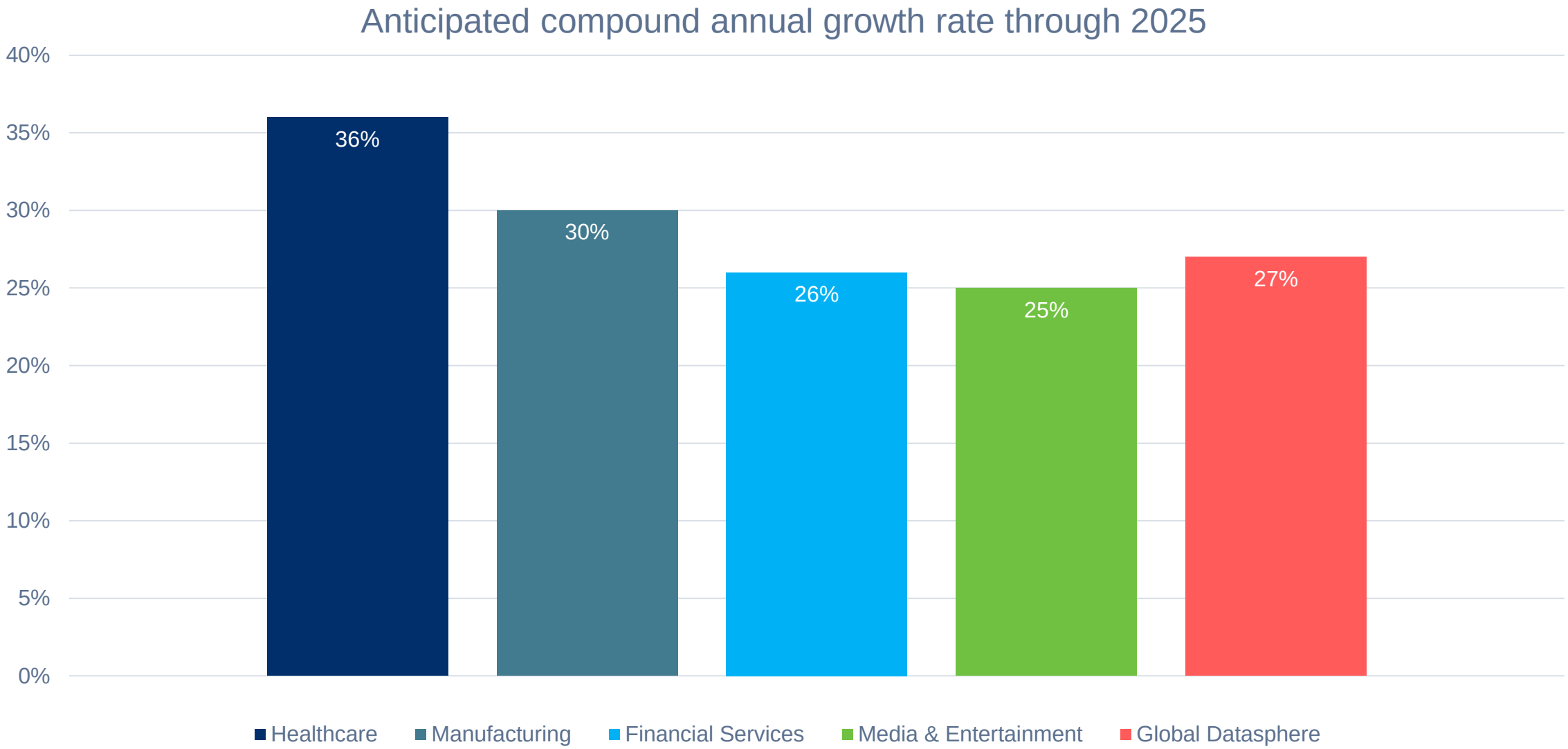


The sheer volume of healthcare data is growing at an astronomical rate:

153 exabytes (one exabyte = one billion gigabytes) were produced in 2013, and an estimated 2,314 exabytes would be produced in 2020, translating to an overall rate of increase at least 48% annually.

IDC. (2014, April). The digital universe of opportunities: Rich data and the increasing value of the internet of things. Retrieved from https://www.iotjournaal.nl/wp-content/uploads/2017/01/idc-digital-universe-2014.pdf; Petrov, C. (2021, March 18). 25+ impressive big data statistics for 2020. Techjury. Retrieved from https://techjury.net/blog/big-data-statistics/

Healthcare data explosion



IDC. (2018, November). The digitization of the world from edge to core (white paper). Retrieved from https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Failure of healthcare organizations to prioritize cybersecurity

- Focus on complying with regulatory requirements, such as HIPAA and HITECH Act, versus focusing on their specific needs and vulnerabilities
- Senior leadership/board lack full understanding of the risks and/or consequences of inadequate cybersecurity, which leads to lower prioritization
- Budget and resources are affected by leadership's lack of understanding of the threat and desire to focus on meeting requirements versus needs-based approach
- Outsourcing to multiple IT security service providers

HITECH Act: Health Information Technology for Economic and Clinical Health Act

Abel, R. (2019, June 12). Medical cybersecurity execs may have priorities misplaced study. *SC Media*. Retrieved from https://www.scmagazine.com/home/health-care/medical-cybersecurity-execs-may-have-priorities-misplaced-study/; Gunther, R. (2019, March 19). Is cybersecurity a priority In healthcare? *Healthcare IT Today*. Retrieved from https://www.healthcareittoday.com/2019/03/19/is-cybersecurity-a-priority-in-healthcare

Failure of healthcare organizations to prioritize training

Healthcare workers not receiving cybersecurity training

- In an online survey of 1,700 healthcare workers, including physicians, care providers, administrative and IT staff, 25% said they never went through training conducted by their workplace, but believed they should have.
- 34% of the respondents indicated that they were not aware of the cybersecurity policy at their own workplace.

Rosenfeld, S. (2019, August 20). Cybersecurity training not a priority for health systems, employees aren't being trained. *Chief Healthcare Executive*. Retrieved from https://www.idigitalhealth.com/news/cybersecurity-training-not-a-priority-for-health-systems

Summary

- With our ever increasing dependence on technology comes an increased exposure to cyber events that represent a frequent, serious, and costly risk to healthcare practices and facilities.
- Gaining an understanding of the landscape, terminology, and the impact associated with cyber events, we can set the framework for making informed decisions as to the level of vulnerability of your respective practices or organizations.
- Cyber events will often result in cyber liability claims that often involve multiple contributing factors and staff. Strategies to address the issues from which the claims arose should first focus on the most common threats and whether your office has basic policies and procedures to address those threats.

MedPro Group resources

- 10 Ways to Establish a Security Culture at Your Healthcare Organization
https://www.medpro.com/security-culture

- Cybersecurity Risk Resources List
https://www.medpro.com/documents/10502/2824311/Risk+Resources_Cybersecurity.pdf

- The Frontline: Cybersecurity Training for Healthcare Workers
https://www.medpro.com/cybersecurity-training-for-healthcare-workers

- Using Physical Safeguards to Prevent Security Breaches
https://www.medpro.com/documents/10502/3667697/Using+Physical+Safeguards+to+Prevent+Security+Breaches.pdf

- Using Technology-Based Safeguards to Prevent Security Breaches
https://www.medpro.com/documents/10502/3667697/Using+Technology-Based+Safeguards+to+Prevent+Security+Breaches.pdf

More resources are available at www.medpro.com/dynamic-risk-tools

Other valuable resources

- Department of Health & Human Services: Top 10 Tips for Cybersecurity in Health Care https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

- Healthcare Industry Cybersecurity Practices: Managing Threats and Protecting Patients https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx This link will take you to a web page that lists several great resources. Physician practices should click on this link Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

- American Medical Association https://www.ama-assn.org/topics/cybersecurity

- American Dental Association: It appears that ADA's cybersecurity resources are contained within the members only section. You can access the ADA, type cybersecurity in the search engine, and it will take you to publically available information or click this link https://www.ada.org/en/search-results#q=cybersecurity&t=all&sort=relevancy

Disclaimer

The information contained herein and presented by the speaker is based on sources believed to be accurate at the time they were referenced. The speaker has made a reasonable effort to ensure the accuracy of the information presented; however, no warranty or representation is made as to such accuracy. The speaker is not engaged in rendering legal or other professional services. The information contained herein does not constitute legal or medical advice and should not be construed as rules or establishing a standard of care. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, if legal advice or other expert legal assistance is required, the services of an attorney or other competent legal professional should be sought.