LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Insider Threats in Healthcare

04/21/2022

TLP: WHITE, ID# ***202204211300***

Agenda

- What is an Insider Threat?
- Types of Insider Threats
- Key Risks & Challenges of Insider Threats
- Insider Attack Risk Factors
- Indicators of Malicious Insiders
- Progression of an Insider
- Real World Examples of Insider Threats
- How to Prevent an Insider Attack?
- How to Detect & Respond to Insider Threats
- Mitigating Insider Threats

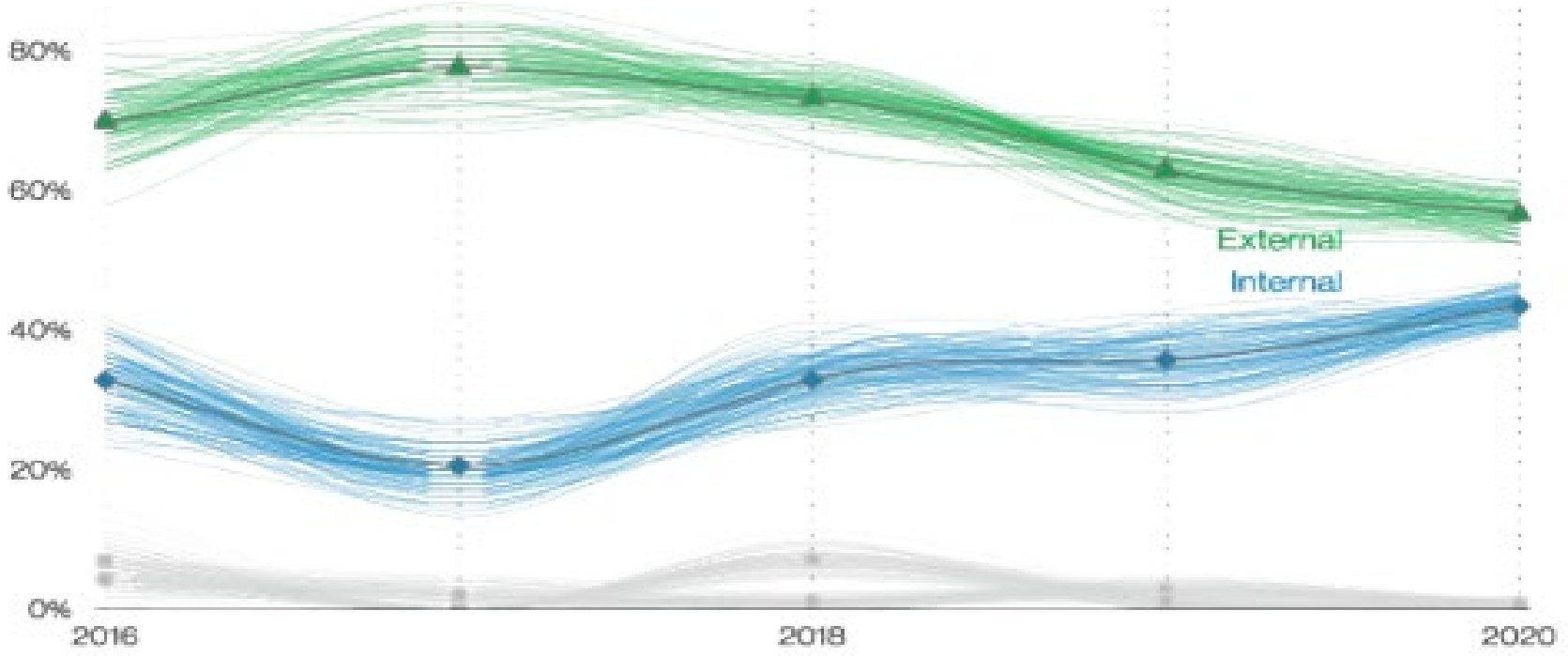
Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What Is an Insider Threat?

An insider threat in the Healthcare and Public Health (HPH) Sector is potentially a person within a healthcare organization, or a contractor, who has access to assets or inside information concerning the organization's security practices, data, and computer systems. The person could use this information in a way that negatively impacts the organization.



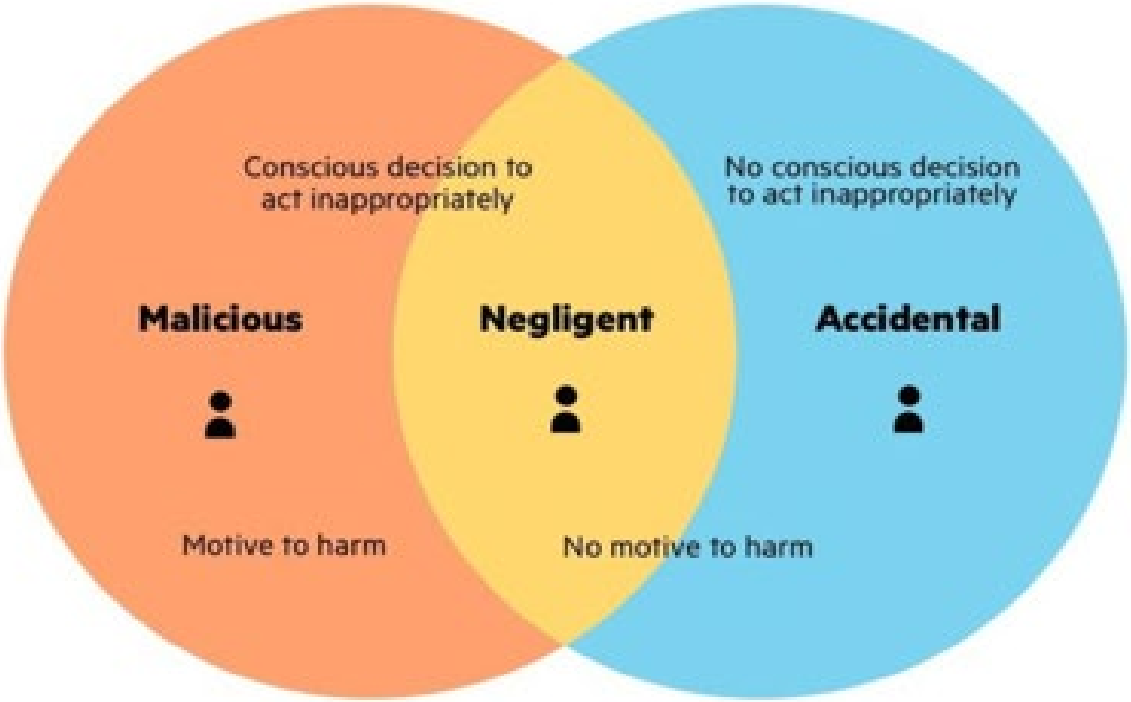
Internal actors' breaches over time

Source: Verizon 2021 Data Breach Report

Types of Insider Threats?

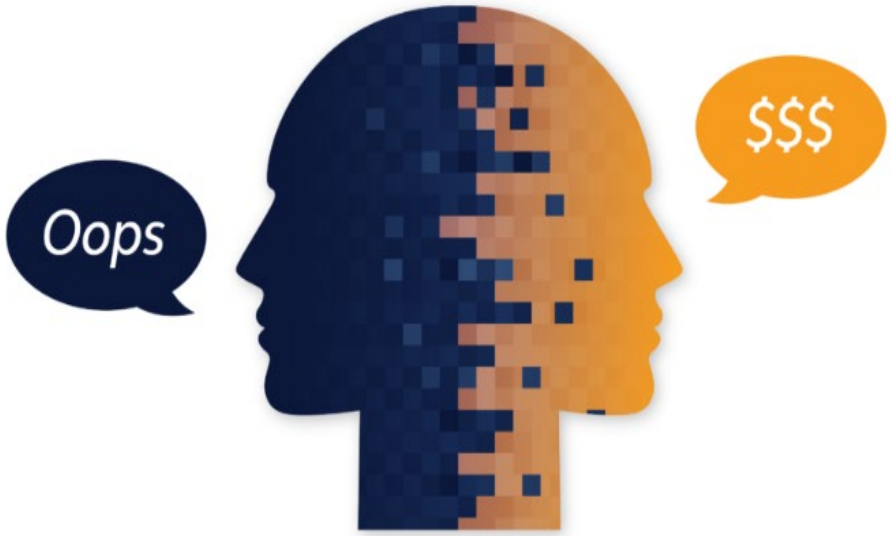
There are several types of insider threats within an organization, all with different goals. Some insider threats are as follows:

- Careless or negligent workers
- Malicious insiders
- Inside agents
- Disgruntled employees
- Third parties



While most companies invest more money on insider threats with malicious intent, negligent insider threats are more common. According to Ponemon's *2020 Insider Threats Report*, 61% of data breaches involving an insider are primarily unintentional, caused by negligent insiders.

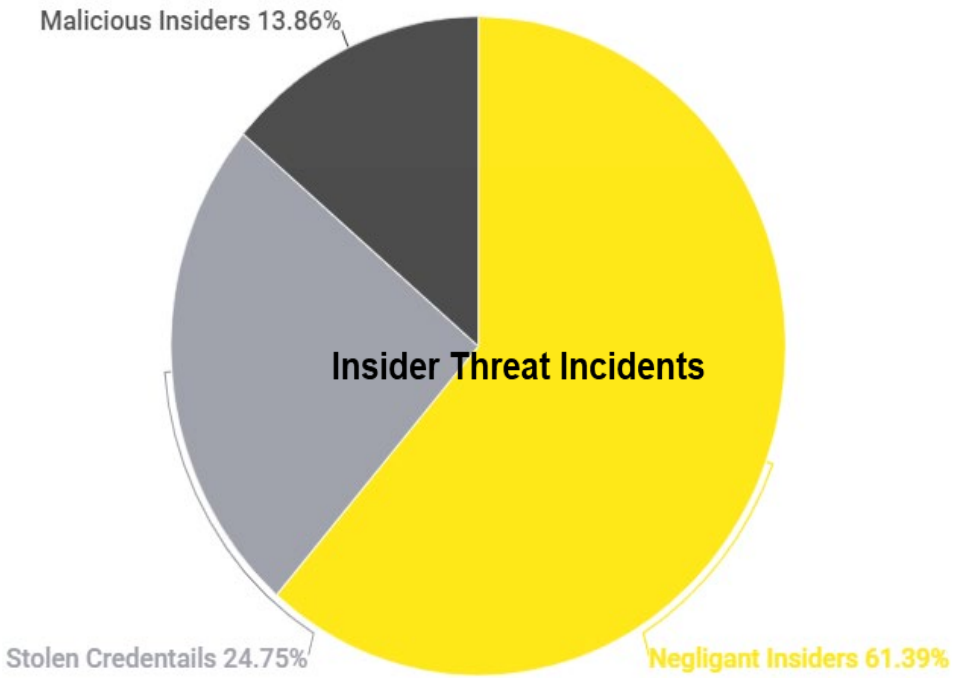
- Lack of awareness about security policies and a failure to provide security awareness training
- 27% of employees saw security policies less than once a year; 39% received security awareness training less than once a year
- Unintentional insider threats pose a major risk to the health sector
- An example is an employee leaving an unencrypted mobile device or laptop containing sensitive data unattended. The device(s) could be stolen, or data could be copied while the device is unattended.
- Alexa on while sensitive meetings are going on (i.e., working remote) could cause sensitive data to be leaked



Malicious Insiders

Malicious insiders are insiders that have a grievance against a company and choose to act on it. While more money is allocated to protect against these type of threats, studies show they pose less of a threat to organizations than insider threats. It is important to mention that there are different studies on this with varied metrics. According to the Ponemon Institute's *2020 Insider Threats Report*:

- Malicious Insiders – 14% of Insider Threat Incidents
- Negligent Insiders – 61% of Insider Threat Incidents
- Negligent Insiders (credentials stolen) – 25% of Insider Threat Incidents



This type of insider threat works on behalf of an external group to compromise an organization's network and carry out a data breach or other attack. This is dangerous because it provides an outside group with the access and privileges of an insider.

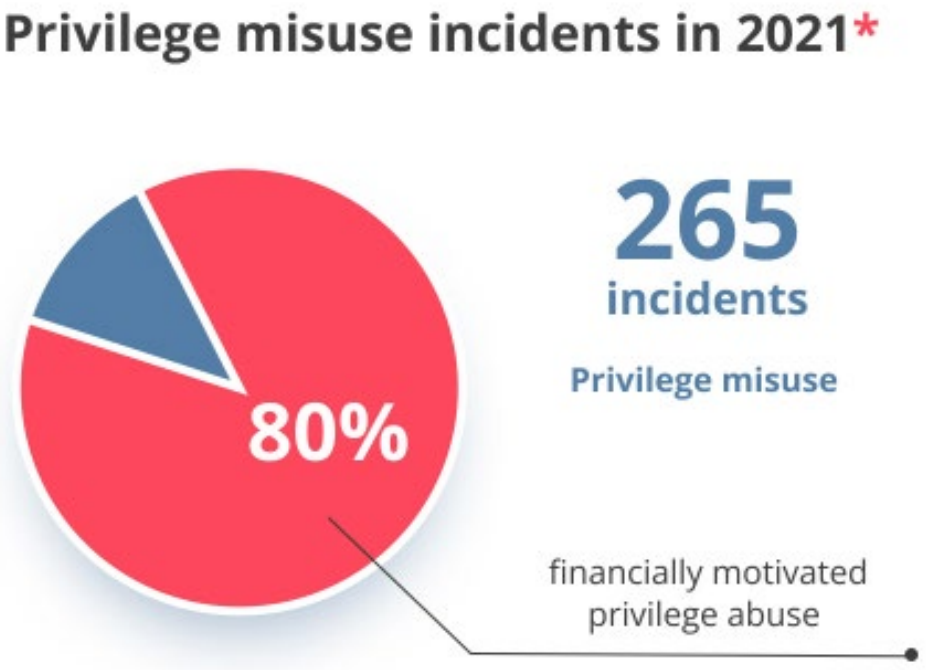
Insider Threat Damage

Percentage of Common Types of Insider Threat Damage

Critical data loss	40%	Legal liabilities	21%
Operational outage/disruption	33%	Expenses on remediating intrusions	19%
Brand damage	26%	Competitive loss	17%

Disgruntled employees can be a significant threat because of their access to systems. They are considered emotional threat actors with an intent to cause harm to their company, and in some cases feel as is they are owed something.

According to CERT, an employee normally becomes disgruntled due to an unmet expectation or an unfortunate event. In Verizon's 2021 Data Breach Report, 80% of privilege misuse was financially motivated.



- Insider threats are not just internal employees but can also take the form of third parties.
- 94% of organizations give third parties access to their systems.
- In 72% of case studies, third party vendors were provided elevated permissions on these systems.

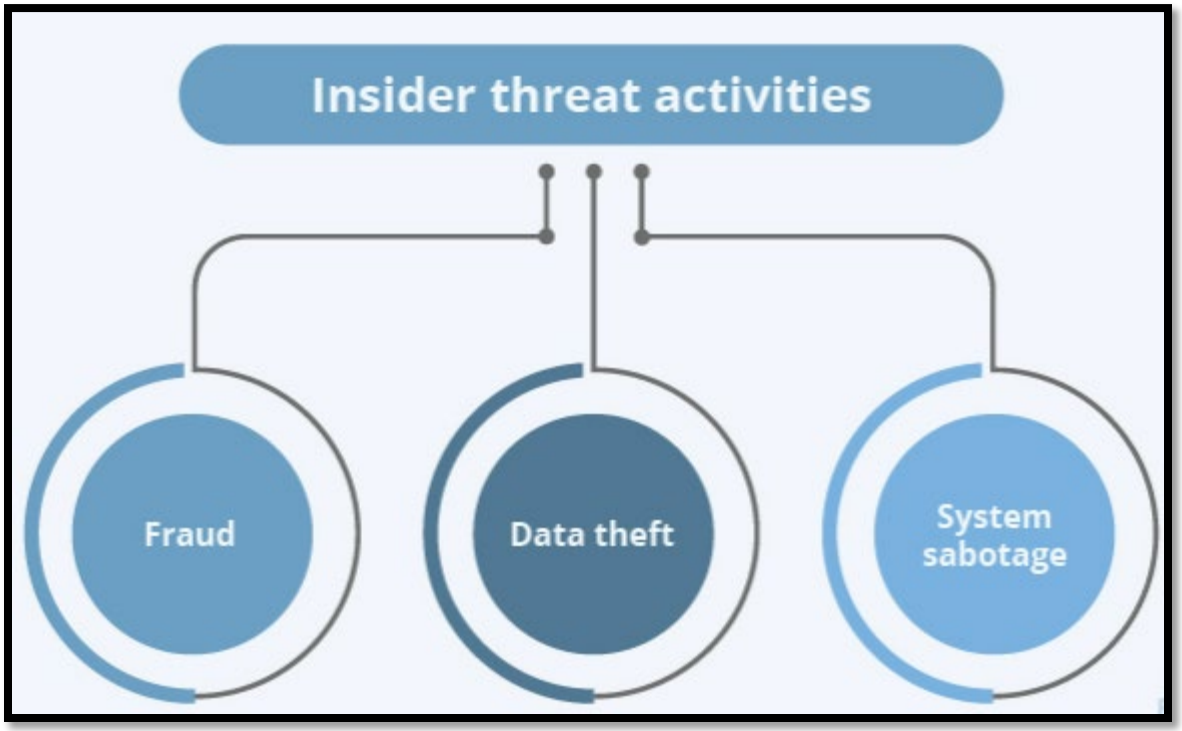
The chart below from Varonis shows how much healthcare data was compromised in 2021. The average TB contains 1.3 million files. Assessing risk per terabyte provides a clearer picture of the typical attack surface by organization size and reveals which ones are most vulnerable to insider and outsider threats.

State of Data Per Terabyte: Healthcare

Organization size	Files	Folders	Exposed folders	Exposed files	Uniquely permissioned folders	Exposed sensitive files	Stale, sensitive files	Unresolved SIDs[2]	Folders with inconsistent permissions	Number of reports analyzed	TB analyzed per company
Large	1,550,171	157,569	33,457	13,108	12,587	993	8,136	999	1,497	32	52
Medium	1,716,089	178,935	28,091	19,611	11,330	1,966	13,114	1,348	1,003	22	45
Small	919,923	51,774	10,888	11,888	10,474	5,107	6,425	502	851	4	56
Average	1,569,640	158,377	29,865	15,490	11,965	1,646	9,906	1,097	1,265	58	50

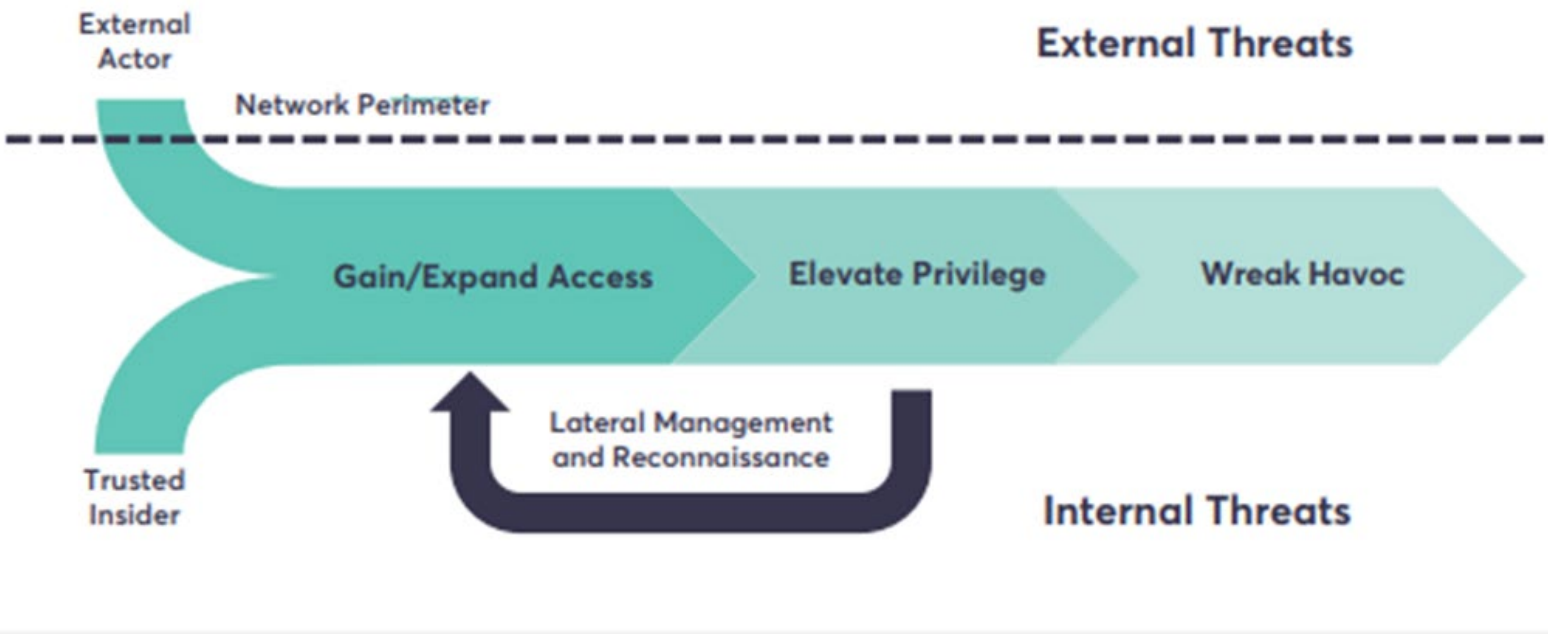
Some risks and challenges the health sector faces because of insider threats are:

- Fraud
- Data theft
- System sabotage



Some Insider attack risk factors are:

- Mismanaged access
- Shadow IT
- Bring Your Own Device (BYOD)



A potential insider threat can be detected through suspicious behavior and various indicators that raise red flags of nefarious activity. Some indicators of malicious activity from an insider are as follows:

Behavioral indicators

- Official records of security violations or crimes
- Cases of unprofessional behavior
- Cases of bullying other employees
- Personality conflicts
- Misuse of travel, time, or expenses
- Conflicts with coworkers or supervisors

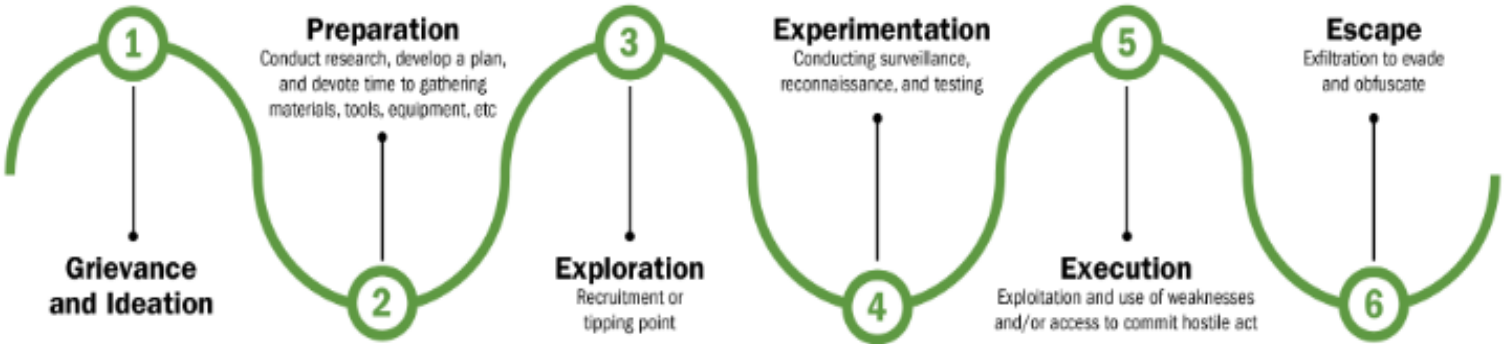
Indicators of IT sabotage

- Creating backdoor accounts
- Changing all passwords so that nobody can access data
- Disabling system logs
- Installing a remote network administration tool
- Installing malware
- Accessing systems or machines of other employees

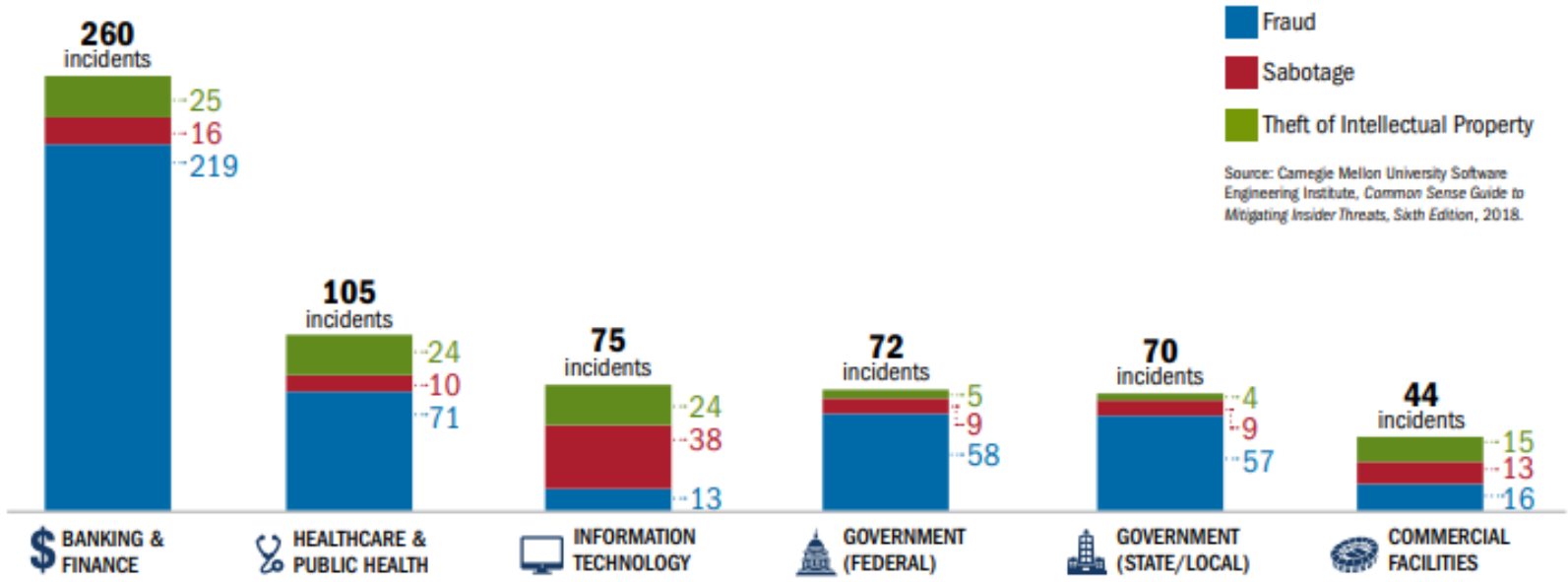
Indicators of data theft

- Massive downloading of corporate data
- Sending sensitive data to a non-corporate address
- Sending emails with heavy attachments to non-corporate addresses
- Extensive use of corporate printers
- Remotely accessing a server during non-working hours

Progression of an Insider (Toward a Malicious Incident)



Top Six Sectors for Fraud, Sabotage, and Theft of Intellectual Property

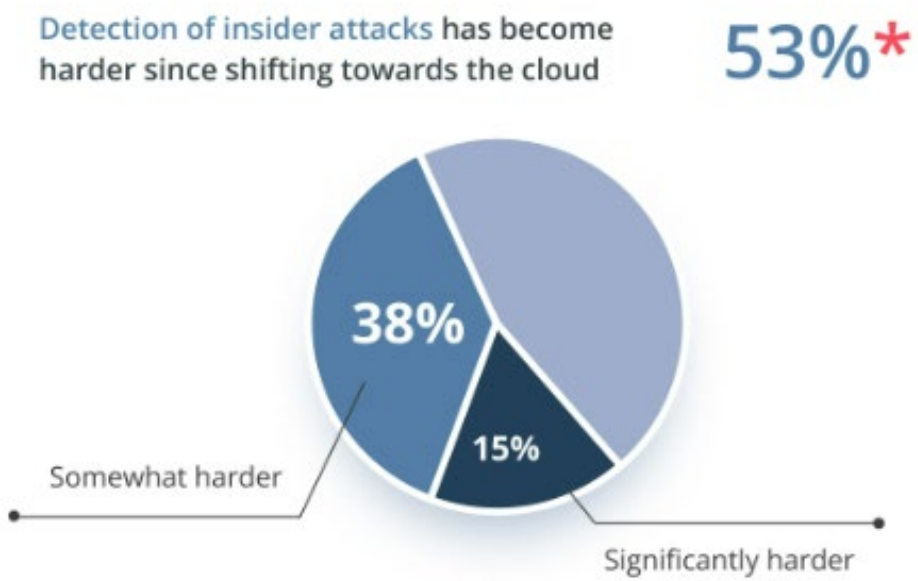


Real World Examples of Insider Threats

Varonis' *2021 Healthcare Data Risk Report* analyzed a random sample of data risk assessments for 3 billion files from 58 companies to show how data is exposed and at risk. The alarming results show:

- Every employee had access to **20%** of all files.
- **31,000 sensitive healthcare files** were open to everyone.
- More than **1 in 10 sensitive files** are open to **every employee.**
- **77%** of companies have **500 or more accounts** with passwords that do not expire.
- Shifting toward cloud services made insider threats **53%** harder to detect.

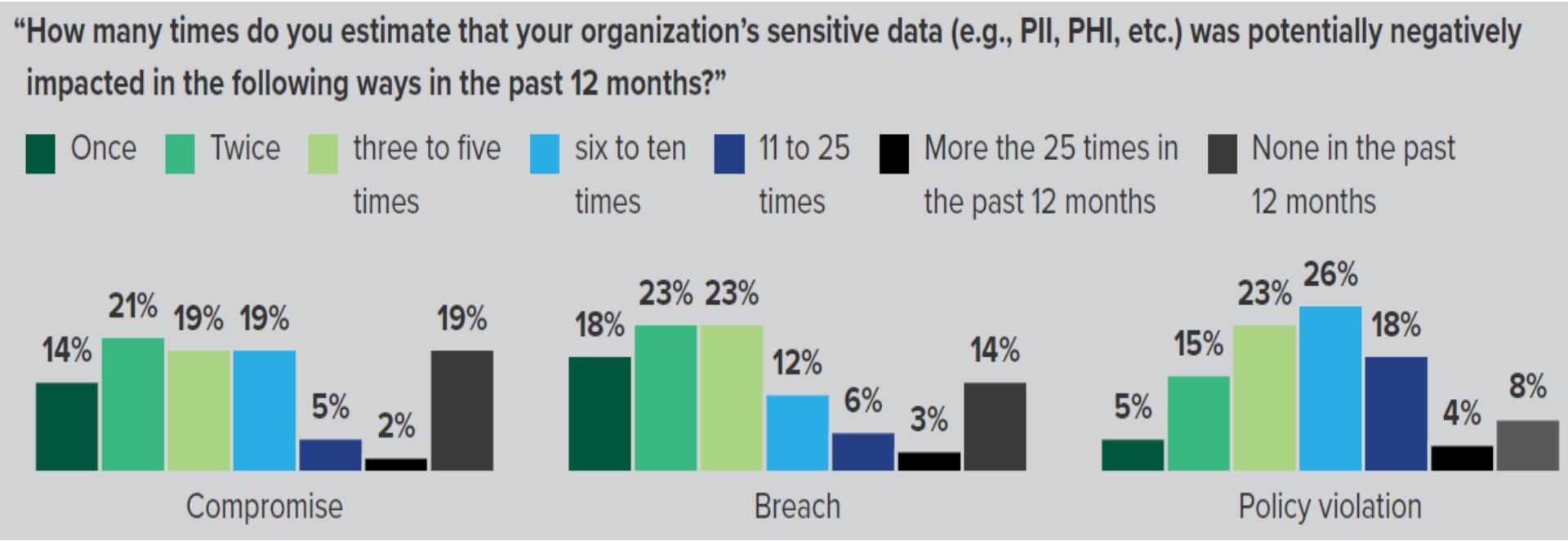
- In October 2021, a major U.S. pharmaceutical company launched an investigation after an employee downloaded 12,000 confidential files on a cloud system before leaving to work for their competitor.
- A Texas hospital employee filmed himself infiltrating the hospital network and creating a backdoor in a HVAC unit that could impact medicine and patients if the system shut down.



Real World Examples of Insider Threats, Part II

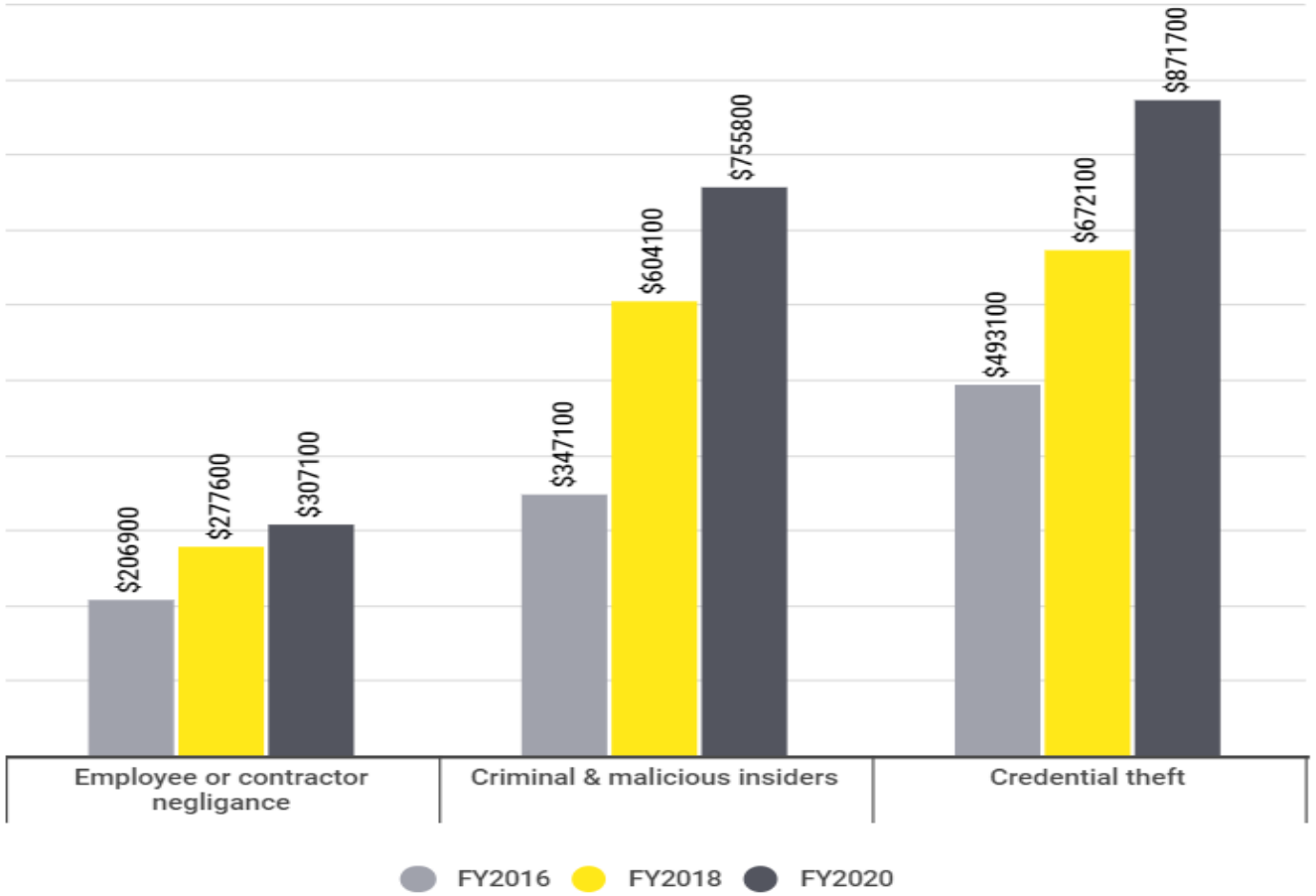
In a 2021 survey conducted by Forrester, almost one quarter of survey respondents who experienced data breaches included at least one insider threat. The chart below breaks this up into three categories: Compromise, Breach, and Policy Violation.

In March 2022, there were 30 healthcare data breaches, with 1.4 million victims reported to the HHS.



Average Cost of Insider Threats Per Incident (U.S. Dollars)

According to the Ponemon Institute's *2020 Cost of Insider Threats*, global organizations reported that the annual costs of insider threats is $11.45 million. This chart shows the average cost per incident from 2016-2020:



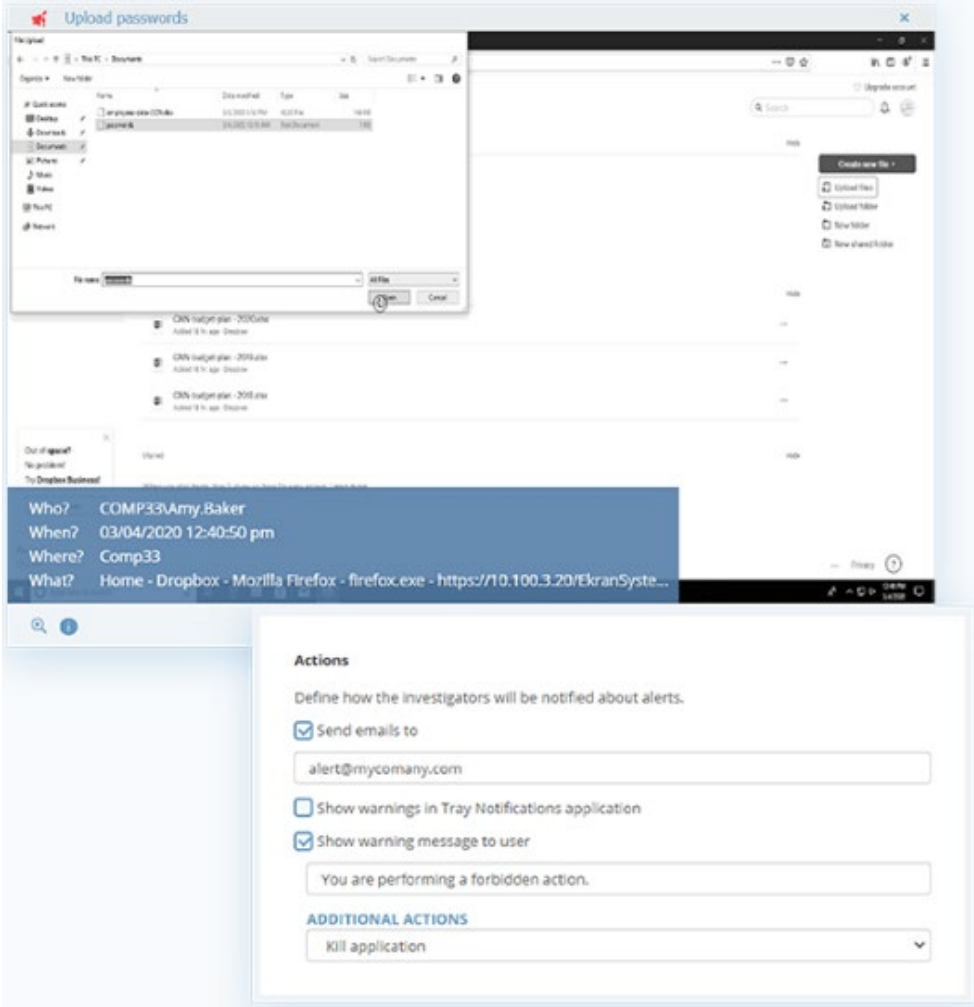
Source: Ponemon Institute 2020 Cost of Insider Threats Report

Deterrence, detection analysis, and post-breach forensics are key areas of insider threat prevention. Here are some additional critical areas we recommend healthcare organizations focus on to prevent insider threats:

- Revise and update cybersecurity policies and guidelines
- Limit privileged access and establish role-based access control
- Implement the zero-trust and MFA models
- Back up data and deploy data loss prevention tools
- Manage USB devices across the corporate network

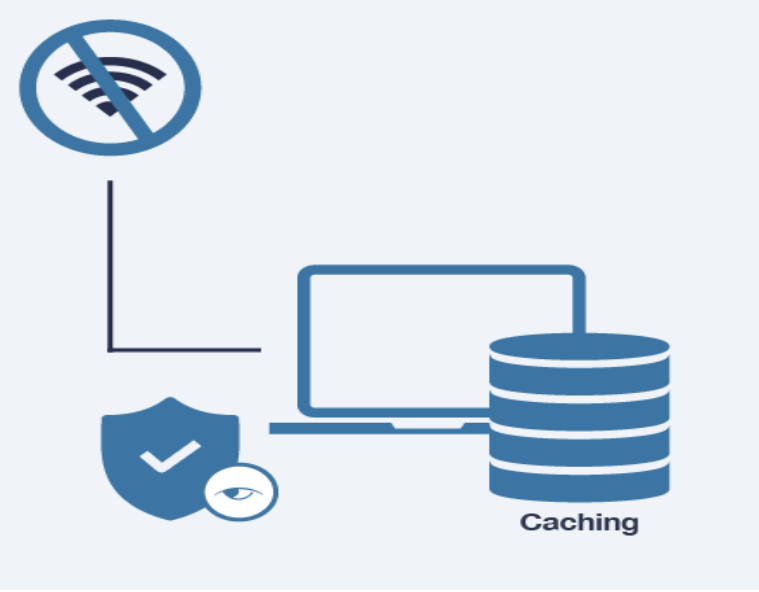
There are several factors that impact an organization's ability to effectively detect and respond to insider threats. They are as follows:

- User Activity Monitoring
- Logging and auditing
- Incident detection and response
- User and Entity Behavior Analytics (UEBA)
- Employee Education



The following best practices for mitigating an insider threat:

- Incorporate insider threat awareness into periodic security training for all employees.
- Implement strict password and account management policies and practices.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Ensure that sensitive information is available only to those who require access to it.
- Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
- Develop a formal insider threat mitigation program.



There are various types of insider threats, and the best approach for any organization is to be proactive, stay vigilant, have a plan, and implement recommendations made in this presentation where needed.

CISA offers free cybersecurity services and tools, along with pertinent guidelines and updates that can help large and small organizations in the health sector. This information can be accessed online at www.cisa.gov/free-cybersecurity-services-and-tools.

Identifying an insider threat should be a team effort between healthcare leadership, IT and the Human Resources department. This will help organizations implement targeted monitoring and detect malicious insiders in a timely manner, hopefully before they cause damage.

Reference Materials

References

- “31 Insider Threat Stats You Need To Know In 2022,” Soft Activity, Monitoring Software Blog. January 7, 2021. https://www.softactivity.com/ideas/insider-threat-statistics/ .
- “Poor Employee Cyber Hygiene is Putting Healthcare Cybersecurity at Risk,” HIPAA Journal. March 7, 2022. https://www.hipaajournal.com/poor-employee-cyber-hygiene-is-putting-healthcare-cybersecurity-at-risk/.
- “5 Levels of User Behavior Monitoring,” Ekran System. August 14, 2019. https://www.ekransystem.com/en/blog/5-levels-user-behavior-monitoring .
- “DBIR 2021 Data Breach Investigations Report,” Verizon. May 13, 2021. https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdfx .
- “Insider Threat Statistics for 2022: Facts and Figures,” Ekran System. March 9, 2022. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures.
- “Detecting and Identifying Insider Threats,” CISA. https://www.cisa.gov/detecting-and-identifying-insider-threats .
- Kaplan, Dan. “3 Ways Automation and Orchestration Can Help You Stem the Insider Threat,” Siemplify. May 30, 2019. https://www.siemplify.co/blog/3-ways-automation-and-orchestration-can-help-you-stem-the-insider-threat/.
- “How to Protect Your Data From Disgruntled Employees,” Data Locker. December 12, 2016. https://datalocker.com/blog/cyberthreats/hacking/how-to-protect-your-data-from-disgruntled-employees/ .

References

- “Portrait of Malicious Insiders: Types, Characteristics, and Indicators,” Ekran System. June 23, 2021. https://www.ekransystem.com/en/blog/portrait-malicious-insiders .
- “Insider Threat Mitigation Guide,” CISA. November 2020. https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf .
- “2021 Data Risk Report: Healthcare, Pharmaceutical, & Biotech,” Varonis. March 29, 2021. https://info.varonis.com/hubfs/Files/docs/research_reports/2021-Healthcare-Data-Risk-Report.pdf.
- “The insider risk within Healthcare,” Security Magazine. April 1, 2021. https://www.securitymagazine.com/articles/94938-the-insider-risk-within-healthcare.
- “Insider Threats: In the Healthcare Sector,” Center for Internet Security. https://www.cisecurity.org/insights/blog/insider-threats-in-the-healthcare-sector .
- “5 Types of Insider Threats in Healthcare – and How to Mitigate Them,” Imprivata. March 28, 2019. https://www.imprivata.com/blog/5-types-of-insider-threats-in-healthcare-and-how-to-mitigate-them .
- Gatlan, Sergiu. “US national emergency extended due to elevated malicious cyber activity,” Bleeping Computer. March 30, 2022. https://www.bleepingcomputer.com/news/security/us-national-emergency-extended-due-to-elevated-malicious-cyber-activity/ .
- “Insider Threat and How to Mitigate It – 5 Top Tips,” FTI Consulting. September 24,2020. https://www.fticonsulting.com/emea/insights/fti-journal/covid-19-how-mitigate-insider-threat / .

Questions

Upcoming Briefs

- 5/5 – Ransomware Trends in the HPH Sector for Q1 2022

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV