LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Quantitative Risk Management for Healthcare Cybersecurity

05/07/2020

Report #: 202005071030

Agenda

- Risk Management
- Risk Frameworks
- Qualitative Vs. Quantitative Risk Management
- Quantitative Approach Over Qualitative Measures
- Traditional Risk Management and the Way Forward
- Cyber Risk
- Data Needed for Quantitative Risk Management
- Examples of Quantitative Approaches
- Key Risk Indicators (KRIs)
- Some Metrics Used in Quantitative Risk Management
- Small Healthcare Organization Usage
- Case Study: Mayo Clinic Supply Chain Risk Management
- Data Breaches from 2019 Verizon Data Breach Investigation Report
- Legislation, Regulations and Standards

Slides Key:

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

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

Risk Management

- What is risk management?
  - The process of identifying potential exposure to weakness or threats to failure of an organization's ability to complete its goals.
  - Risk management is used to reduce uncertainty in support of good decision making
  - There are many models with four or more steps- it's a continuous process
  - Most risk management methodologies/models include the following:
    - Identification of risk
    - Analysis of risk
    - Risk mitigation
      - Accept
      - Avoid
      - Transfer
      - Reduce
    - Monitoring and control of residual risk

Image source: Agileaces.net

Risk Frameworks

- Frameworks for developing risk metrics include risk models such as the general model offered by NIST SP 800-30R1 (NIST 2012).
- NIST Cybersecurity Framework includes three components:
  - **Core:** Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls
    - Identify – Risk assessment, asset management, supply chain risk management
    - Protect - Identity and access control, awareness training, data security
    - Detect – Continuous monitoring
    - Respond – Mitigation, response planning, analysis
    - Recover – Recovery planning, improvements
  - **Profiles:** Alignment of an organization's requirements and objectives, risk appetite and resources using the desired outcomes of the Framework Core
  - **Implementation Tiers:** A qualitative measure of organizational cybersecurity risk management practices

Image Source: NIST

National Institute of Standards and Technology. (November 18, 2019). Framework V1.1 Slide Presentation. NIST. Accessed April 24, 2020 at: https://www.nist.gov/cyberframework/new-framework#background

Qualitative vs. Quantitative Risk Management

- Qualitative Defined
  - Qualitative measures seek to define risk in terms of severity, impact, and likelihood of occurrence with precision levels of “low,” “medium,” and “high.”
  - They are typically cheaper and faster to implement because they are not numerically based.

- Quantitative Defined
  - Quantification is “the expression or measurement of the quantity of something” which when applied to cyber risk can help us break down risk into distinct aspects that are able to be measured.

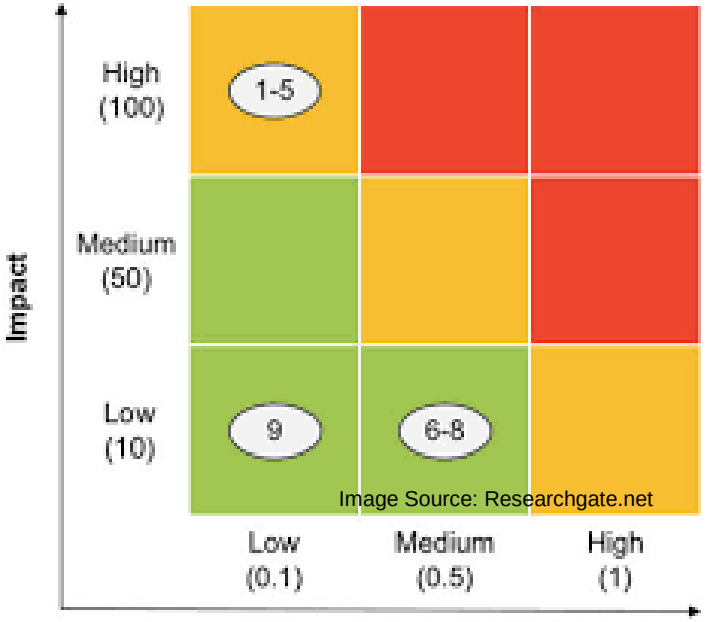

Image Source: Researchgate.net

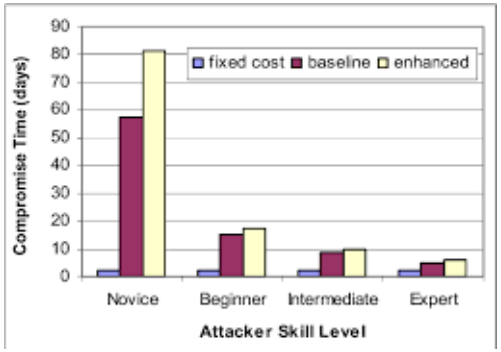

Image Source: Semanticscholar.org

Graves, R. (2000). Qualitative risk assessment. *PM Network, 14*(10), 61–66.
Sanna, N. (November 15, 2019). “What is Cyber Risk Quantification?” RiskLens.com. Accessed April 22, 2020 at: https://www.risklens.com/blog/what-is-cyber-risk-quantification/

Quantitative Approach over Qualitative Measures

There are several reasons to choose a quantitative approach over qualitative ones.

Risks to using qualitative measures:

- Subjective
- Lack transparency
- Lack reproducibility
- Getting reversed risk rankings
- Uninformative ratings
- Zero value of information (VOI)

Leveraging a quantitative approach:

- Transparent
- Repeatable
- Scalable
- Reproducible

- Can easily prioritize high risks in organization
- Can build out trendlines of high risk items
- Enables aggregation of multiple high risk rated items
- Can perform cost-benefit analysis
- More effectively manage organizational risk appetite
- Ensures consistency of ratings and facilitates benchmarking against industry or peers
- Assists in determining how much risk-based capital to budget for

Cox, L. Djangir Babayev, William Huber. (June 9, 2005). Some Limitations of Qualitative Risk Rating Systems. Risk Analysis, 25:3. Accessed April 27, 2020 at: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2005.00615.x.
Freund, J. (June 19, 2019). "Gartner 2019 Debate: Quantitative vs. Qualitative Cyber Risk Analysis." RiskLens.com. Accessed April 23, 2020 at: https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/

Traditional Risk Management and the Way Forward

Traditional risk management approaches often use qualitative measurements with ordinal scales from 1 – 10, or High, Medium, and Low classifiers, which can be subjective or ineffective.

Challenges – Quantitative	Challenges - Qualitative
• Some organizations do not know where their critical systems or data are, so risk values would not be truly accurate	• 70% Organizational leadership surveys cite qualitative measures are difficult to understand and/or not helpful
• Can be a struggle to come up with risk values	• Risk values are not always defendable

Freund, J. (June 19, 2019). "Gartner 2019 Debate: Quantitative vs. Qualitative Cyber Risk Analysis." RiskLens.com. Accessed April 23, 2020 at: https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/

Cyber Risk

- Risk management principles seek to reduce uncertainty and exposure.
- Government, regulators, and board rooms are looking for cyber risk to be communicated in business language.
- Risk can be defined as “the probable frequency and probable magnitude of future loss” that is associated with a specific event or set of circumstances.
- In order to describe risk scenarios, the asset of value needs to be defined, the threat identified, the effect of the threat, and the resulting impact discussed.

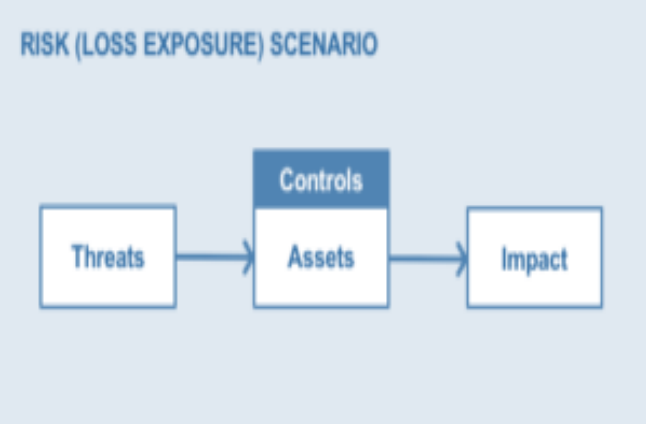

Image Source: RiskLens

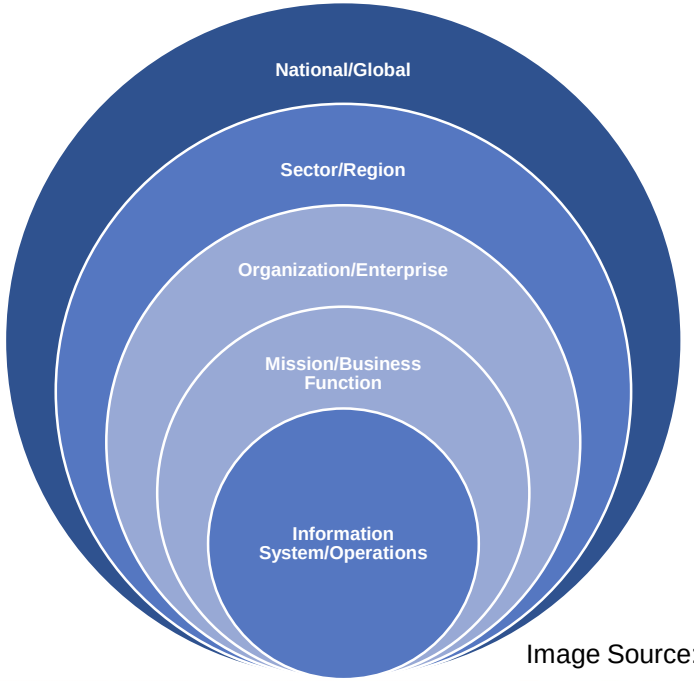

Image Source: HSSEDI

Data Needed for Quantitative Risk Management

Cyber risk management policies may align to risk management frameworks such as NIST Cybersecurity Framework (CSF)

- Voluntary
- Built as a collaboration between the public and private sector based on best practices

To quantify cyber risk:

- Systems and data inventory should be performed in order to account for assets, and also definitively identify the location of organizational “crown jewels”

Risk = Vulnerability x Threat x Asset Value x Probability of Occurrence

NIST. (November 18, 2019). “Cybersecurity Framework.” NIST. Accessed April 24, 2020 at: https://www.nist.gov/cyberframework/new-framework#background
Freund, J. (June 19, 2019). “Gartner 2019 Debate: Quantitative vs. Qualitative Cyber Risk Analysis.” RiskLens.com. Accessed April 23, 2020 at: https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/

Examples of Quantitative Approaches

- Cyber VaR (CVaR)
  - Seeks to assist risk and infosec professionals articulate cyber risk in financial terms, and to enable organizations in making cost-effective decisions balancing the business objectives and the need to protect the organization from cyber threats.
- Factor Analysis of Information Risk (FAIR)
  - FAIR is a CVaR method that accounts for operational and information risk.
- Hubbard and Seiersen (H&S) Approach
  - Similar to FAIR, this approach quantifies cyber risk through measuring loss event frequency and loss magnitude.

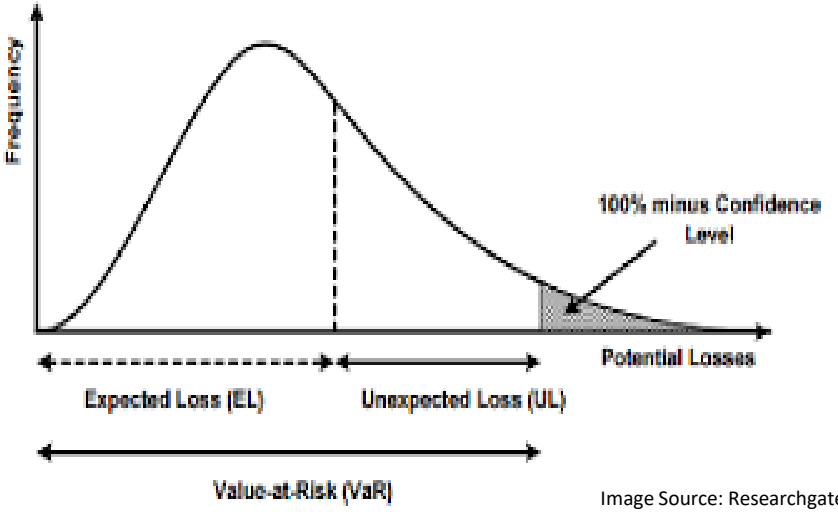

Image Source: Researchgate.net

Jones, N. and Brian Tivnan. (May 11, 2018). Cyber Risk Metrics Survey, Assessment, and Implementation Plan. The Homeland Security Systems Engineering and Development Institute (HSSEDI) Operated by the MITREE Corporation. Accessed April 25, 2020 at: https://www.mitre.org/sites/default/files/publications/pr_18-1246-ngci-cyber-risk-metrics-survey-assessment-and-implementation-plan.pdf

Key Risk Indicators (KRIs)

- Strategic to operational
- Key Risk Indicators (KRIs) are measurements which provide an early signal of increasing risk exposures in various organizational areas.
  - In many cases, Key Performance Indicators (KPIs) can be re-worked into a well-developed KRI and represent a lagging KRI
- Types of KRIs:
  - Leading – Emerging risks
  - Lagging – Trailing
- Examples of KRIs:
  - Percentage of systems in use that are no longer supported – The number of systems currently in use which are no longer supported by the original developer as a percentage of total systems used by the organization at the same point in time. These non-supported systems may also be considered “legacy” systems.
  - Percentage of workstations without a full malware scan within last 24 hours – The number of workstations that have not undergone a full, successful virus scan with that last 24 hours as a percentage of total active workstations managed by the organization.

Jones, N. and Brian Tivnan. (May 11, 2018). Cyber Risk Metrics Survey, Assessment, and Implementation Plan. The Homeland Security Systems Engineering and Development Institute (HSSEDI) Operated by the MITREE Corporation. Accessed April 25, 2020 at: https://www.mitre.org/sites/default/files/publications/pr_18-1246-ngci-cyber-risk-metrics-survey-assessment-and-implementation-plan.pdf

Some Metrics for Quantitative Risk Management

- Basic Calculations that can be used to quantify risk are:
  - Exposure Factor (EF) = the percentage of an asset value that would be lost if the exploit were to occur
  - Asset Value (AV) = the estimated cost of the company's property, reputation, or goodwill that is at risk
  - Annual Rate of Occurrence (ARO) = the amount of times an exploitation is estimated to occur in a year
  - Single Loss Expectancy (SLE) = AV multiplied by the EF
  - Annual Loss Expectancy (ALE) = SLE multiplied by the ARO

Image Source: novuhealth.com

Small Healthcare Organization Usage

Most small healthcare organizations do not have abundant resources or a dedicated employee for Information Technology Security making cybersecurity risk management essential.

Assessment of cybersecurity risk does not have to use complex methods but should help the organization to identify vulnerabilities and allocate its resources by using metrics to determine:

- the likelihood of vulnerabilities being successfully exploited by a threat actor; and
  - Annual Rate of Occurrence (ARO)
  - Exposure Factor (EF)
- the magnitude of the impact on the organization:
  - Single Loss Expectancy (SLE)
  - Annual Loss Expectancy (ALE)

Exploit	Asset value	Exposure Factor	Single loss Expectancy	Annual Rate of Occurrence	Annual Loss Expectancy
Ransomware	$900K	100%	$900K	1	$900K
Data Exfiltration	$150K	75%	$112.5K	3	$337.5K
Privilege Escalation	$50K	50%	$25K	5	$125K

Data is fictional based of cost estimates from Healthsecurity.com

Case Study: Mayo Clinic Supply Chain

In NIST Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic

The study detailed how the Mayo Clinic:

- Partners with its vendors to improve the cybersecurity of medical/research devices
- Requires that vendors complete an extensive security assessment before being accepted into the supply chain
- Conducts in-depth manual security assessment into the vendor that highlights
  - outstanding vulnerabilities
  - appropriate remediation plans and
  - timelines to resolve the issues.
- Identifies risks that may be introduced into the patient care environment by the vendor which can be addressed by collaborative mitigation strategies.

Data Breaches from 2019 Verizon Data Breach Investigation Report

Healthcare stands out due to the majority of breaches being associated with internal actors. Denial of Service attacks are infrequent, but availability issues arise in the form of ransomware.

Frequency	466 incidents, 304 with confirmed data disclosure
Top 3 patterns	(1) Miscellaneous Errors, (2) Privilege Misuse and (3) Web Applications represent 81% of incidents within Healthcare
Threat actors	• Internal (59%), • External (42%), • Partner (4%), and • Multiple parties (3%) (breaches)
Actor motives	• Financial (83%), • Fun (6%), • Convenience (3%), • Grudge (3%), • and Espionage (2%) (breaches)
Data compromised	• Medical (72%), • Personal (34%), • Credentials (25%) (breaches)

Legislation, Regulations and Standards

There are many Government documents that provide guidance on risk management and although they often are addressing federal agencies many of the concepts can be applied to the private sector.

- The National Institute of Standards and Technology (NIST) has several special publications that address Risk Management:
  - NIST SP 800-39 - Managing Information Security Risk
  - NIST SP 800-30 – A guide to conducting Risk assessments
  - NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST SP 800-66 - An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

- The Health and Human Services also has several documents specific to the Healthcare Sector:
  - HHS, Office of Civil Rights - Guidance on Risk Analysis Requirements under the HIPAA Security Rule
  - HHS, Office of Civil Rights - HIPAA Compliance Checklist
  - HHS, CMS – Basics of Risk Analysis and Risk Management
  - HHS, Health Information Technology – Guide to privacy and security of Electronic Health Information
  - HHS, Public Health Emergencies - Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Legislation, Regulations and Standards Cont.

Additionally, other institutions provide guidance on Cybersecurity Risk Management in the Healthcare Industry:

- Verizon – 2019 Data Breach Investigations Report, Healthcare Section
- The MITRE Corporation – Risk Management
- The MITRE Corporation – Risk Management Tools
- The MITRE Corporation – Risk Impact Assessment and Prioritization

Reference Materials

References

- SOME LIMITATIONS OF QUALITATIVE RISK RATING SYSTEMS. RISK ANALYSIS, 25:3.
  - https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2005.00615.x.
- GARTNER 2019 DEBATE: QUANTITATIVE VS. QUALITATIVE CYBER RISK ANALYSIS.
  - https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/
- QUALITATIVE RISK ASSESSMENT.
  - https://www.pmi.org/learning/library/qualitative-risk-assessment-cheaper-faster-3188
- MITRE ATT&CKCON 2.0
  - https://attack.mitre.org/resources/attackcon/
- A METHOD FOR QUANTITATIVE RISK ANALYSIS
  - https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/p28.pdf
- NIST PRIVACY FRAMEWORK: A TOOL FOR IMPORVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
- CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT: OBSERVATIONS FROM INDUSTRY
  - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-5.pdf
- GUIDE FOR CONDUCTING RISK ASSESSMENTS: INFORMATION SECURITY
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTING (HIPAA) SECURITY RULE
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

References

- SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- SOME LIMITATIONS OF QUALITATIVE RISK RATING SYSTEMS
  - https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2005.00615.x
- METRICS OF SECURITY
  - https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917850
- WHAT IS THE FAIR INSTITUTE?
  - https://www.fairinstitute.org/
- UNDERSTANDING CYBER RISK QUANTIFICATION: THE BUYER'S GUIDE.
  - https://www.fairinstitute.org/blog/download-understanding-cyber-risk-quantification-the-buyers-guide-by-jack-jones
- FAIR ADOPTION SOARS AS 3,000 MEMBERS MILESTONE IS HIT
  - https://www.fairinstitute.org/blog/fair-adoption-soars-as-3000-members-milestone-is-hit
- FAIR RISK MANAGEMENT
  - https://www.fairinstitute.org/fair-risk-management
- INFORMATION SECURITY: AGENCIES NEED TO IMPROVE IMPLEMENTATION OF FEDERAL APPROACH TO SECURING SYSTEMS AND PROTECTING AGAINST INTRUSIONS.
  - https://www.gao.gov/assets/700/696105.pdf
- CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES
  - https://www.gao.gov/assets/710/700503.pdf

References

- CYBERSECURITY: DOD NEEDS TO TAKE DECISIVE ACTIONS TO IMPROVE CYBER HYGIENE.
  - https://www.gao.gov/assets/710/705886.pdf
- TOP 10 TIPS FOR CYBERSECURITY IN HEALTH CARE
  - https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf
- BASICS OF RISK ANALYSIS AND RISK MANAGEMENT
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf
- INFORMATIONSECURITY RISK MANAGEMENT FOR HEALTHCARESYSTEMS
  - https://www.medicalimaging.org/wp-content/uploads/2011/02/Information-Security-Risk-Management-for-Healthcare-Systems.pdf
- RISK MANAGEMENT
  - https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management
- RISK IMPACT ASSESSMENT AND PRIORITIZATION
  - https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-impact-assessment-and-prioritization
- RISK MANAGEMENT TOOLS
  - https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-management-tools
- CYBER RISK METRICS SURVEY, ASSESSMENT, AND IMPLEMENTATION PLAN
  - https://www.mitre.org/sites/default/files/publications/pr_18-1246-ngci-cyber-risk-metrics-survey-assessment-and-implementation-plan.pdf
- NIST CYBERSECURITY FRAMEWORK
  - https://www.nist.gov/cyberframework
- NEW TO FRAMEWORK
  - https://www.nist.gov/cyberframework/new-framework#background

References

- CYBER FRAMEWORK: BACKGROUND
  - https://www.nist.gov/cyberframework/new-framework#background
- TECHNICAL VOLUME 1: CYBERSECURITY PRACTICES FOR SMALL HEALTH CARE ORGANIZATIONS
  - https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf
- GARTNER 2019 DEBATE: QUANTITATIVE VS. QUALITATIVE CYBER RISK ANALYSIS
  - https://www.risklens.com/blog/gartner-2019-debate-quantitative-vs-qualitative-cyber-risk-analysis/
- WHAT IS CYBER RISK QUANTIFICATION?
  - https://www.risklens.com/blog/what-is-cyber-risk-quantification/
- QUANTITATIVE RISK ANALYSIS: YOU HAVE MORE DATA THAN YOU THINK
  - https://www.risklens.com/blog/you-have-more-data-than-you-think/

Questions

Upcoming Briefs

- Foreign Government Targeting of American Healthcare Sector
- Web Shell Malware

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Health Sector Cybersecurity Coordination Center (HC3) Background

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

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently 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 document and presentation that provides 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 call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV