THE HEALTHCARE SECTOR NEEDS A MEASURABLE CYBER RISK PARAMETER: BREACH-LIKELIHOOD

SAFE SCORE WHITEPAPER

www.safe.security

Introduction

Cyber risk is a public health threat

Aligning cybersecurity and patient safety initiatives not only will help your organization protect patient safety and privacy, but will also ensure continuity of effective delivery of high-quality care by mitigating disruptions that can have a negative impact on clinical outcomes. - John Riggi, Senior Advisor for Cybersecurity and Risk, American Hospital Association

Most healthcare organizations assess risk by weighing a data breach's impact on revenue, legal, reputational, and regulatory exposures. Unfortunately, cyberattacks in this sector are not just limited to financial, regulatory or reputational impact; it directly impacts patients.

Universal Health Services (UHS) recently reported losing $67 million after its Ryuk ransomware attack in September 2020. It took three weeks for the organization to get its 400 U.S. health system sites back online. A New England Journal of Medicine study shows that a delay of fewer than five minutes in traffic causes 4% more hospital deaths over the following 30 days - imagine the dire consequences in case of cyber attacks that cripple a healthcare center. In 2019, Israeli researchers showed medical scans vulnerable to fake tumors. In 87% of the cases in which the malware removed cancerous modules, doctors concluded very sick patients were healthy.

If hackers can tamper with CTs or MRIs, it could lead to insurance fraud, ransomware, cyberterrorism, and incorrect surgeries. The American Public Health Association has recognized the growing cyber risk to public health and was joined by 80 other organizations that sent a letter to Congress in May 2019 urging a more robust and comprehensive approach to sector security.

The current attitudes toward cybersecurity must grow beyond the belief that cyber risk can lie solely within the silos of information technology. Cybersecurity is not just an "IT" issue alone.

HISTORICALLY, HACKERS HAVE THREATENED THE CONFIDENTIALITY OF MEDICAL INFORMATION THROUGH DATA BREACHES WHERE THEY OBTAIN SOCIAL SECURITY NUMBERS OR FINANCIAL DATA. BUT IF HACKERS THREATEN THE INTEGRITY OF MEDICAL DATA, SUCH AS BY CHANGING LABORATORY VALUES OR HACKING A REMOTE MEDICAL DEVICE, THAT COULD POSE A VERY REAL DANGER TO PATIENTS"

Rod Piechowski, health IT expert and Vice-President of Thought Advisory at the HIMSS.

89%
of initial compromise in hospitals is still through emails

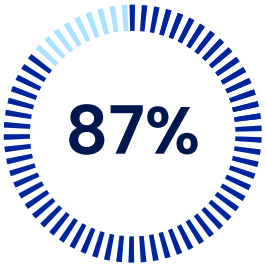
Comparitech analysts estimate that ransomware attacks on US healthcare organizations cost them
US $20B
in 2020 alone.

Hospitals account for
30%
of all significant data breaches.

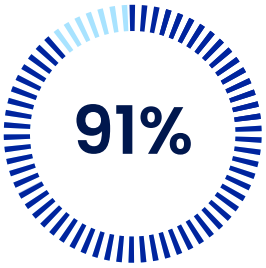
The sector will invest
~$125 billion
in cybersecurity between
2020–25

The cost of ransomware alone has grown by
1094%
since 2015

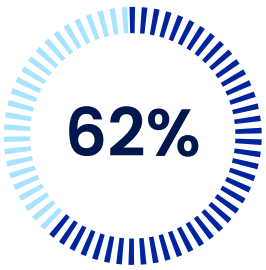
of cyberattacks begin with trusted insiders.



of healthcare IT security leaders say they don't have the right personnel.



of hospital administrators consider cybersecurity as a top priority



of them feel inadequately trained or unprepared to mitigate cyber risks

of U.S. health employees have never received cybersecurity awareness training but felt they should have.

Current cybersecurity practice in the healthcare sector

Cybersecurity is often relegated as a duty of non-medical staff in healthcare organizations. To curb this perspective and build a culture of cybersecurity, a legislatively derived task group, co-led by the AHA, has developed resources on how to incorporate cyber into enterprise risk. In addition, NIST released Draft NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM), to encourage the integration of cybersecurity within enterprise risk management.

Compliance standards are designed to create a specific scope boundary or 'enclave,' limiting its applicability. For instance, compliances may not always protect assets, systems, and functions that are business-critical, even if they are outside of the scope of that enclave. In addition, organizations may still need to implement more dynamic controls to improve their overall security.

While continuous compliance management is the bedrock of cybersecurity in this sector, it also relies on detecting business-critical functions threats rather than predicting the likelihood of breaches. With the rate at which cybercrime is evolving, the regulatory red tape makes it difficult to update regulations fast enough to provide adequate cybersecurity.

Compliance assessment		
Positives	Limitations	
• Objective assessment of specific controls are in place • Heavily Policy Driven • Accepted by Regulator	• Point in Time • Control assessments don't measure risk • Not all controls are of equal importance • None of the control frameworks today take into account the relationships and dependencies between controls.	• Ordinal Values (i.e., labels) - performing math on these values is unreliable • A small Sample set of assets considered for assessing controls

CURRENT CYBERSECURITY PRACTICE IN THE HEALTHCARE SECTOR

CURRENT CYBERSECURITY PRACTICE IN THE HEALTHCARE SECTOR

Risk Matrix (driven by consultants / internal teams)

Positives

- Quick and intuitive
- Relatively low-cost approach

Limitations

- Subjective Interpretations
- Ordinal Values
- Basic math operations
- Point in Time
- Small Sample Set of Assets Considered
- Large Risk variance on the same cell

		Impact				
		Negligible	Minor	Moderate	Critical	Catastrophic
		<$10K	<$10K to <$100K	<$100K to <$1M	<$1M to <$10M	>$10M
Likelihood: Frequent	99%+	Medium	Medium	High	High	High
Likely	>50% - 99%	Medium	Medium	Medium	High	High
Occasional	>25% - 50%	Low	Medium	Medium	Medium	High
Seldom	>1% - 25%	Low	Low	Medium	Medium	Medium
Improbable	<1%	Low	Low	Low	Medium	Medium

Risk A Likelihood is 2%, impact is $10M equals **$200K**

Risk B Likelihood is 20%, impact is $100M equals **$20M**

The products of the likelihoods and impacts of the risks: $200,000 for Risk A (2% × $10 million) and $20 million for Risk B (20% × $100 million).

These two very different risks would actually be plotted in the same cell (that is, same row, same column) on a risk matrix!

CURRENT CYBERSECURITY PRACTICE IN THE HEALTHCARE SECTOR

Risk-Based Vulnerability Management (RBVM)

Positives

- Objective assessment of specific technical controls are in place
- Industry-wide acceptance

Limitations

- Only applicable for vulnerabilities and does not take into account the people and policy element
- No scientific and industry-accepted way to merge various CVSS Scores and CVE IDs together.
- Does not represent an accurate picture when one does not provide Temporal and Environmental Data for the asset
- The score does not depict the likelihood of a breach

Base Metric Group

Exploitability Metrics

Attack Vector

Attack complexity

Privileges Required

User Interaction

Impact Metrics

Confidentiality Impact

Integrity Impact

Required

Attack Vector

Temporal Metric Group

Exploit Code Maturity

Remediation Level

Report Confidence

Environmental Metric Group

Modified Base Metrics

Confidentiality Requirement.

Integrity Requirement.

Availability Requirement

CURRENT CYBERSECURITY PRACTICE IN THE HEALTHCARE SECTOR

Credit-Like Outside in Scoring based on automated external assessment

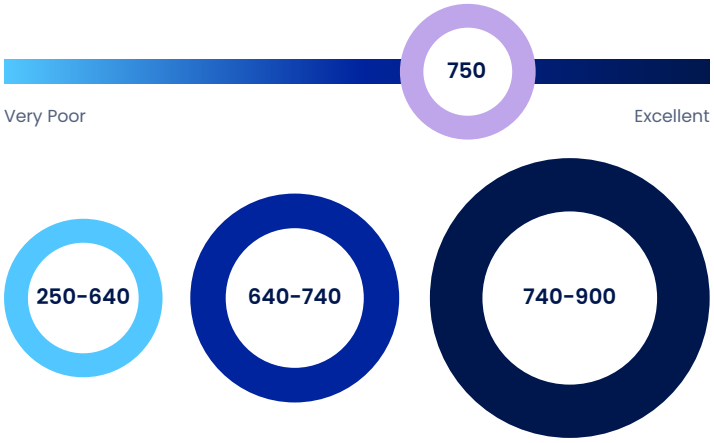
Positives

- Ease of Deployment
- Consultant
- Useful for benchmarking against industry peers
- Easy for Boards and executives to relate to

Limitations

- A significant part of an organisation's risk landscape is not be included as the external digital footprint is generally less then 1% of the total tech stack in an organisation
- In most cases, this gives a false sense of security if you have a good score
- Your security risk posture is publicly disclosed without your consent
- No People, Policy aspect incorporated in the overall scoring

Like Credit Rating



How can cyber risk be measured?

Enterprise Risk is the function of the likelihood of a breach and the business function. Gartner supplements it with the following definition: Cyber Risk Quantification (CRQ) is a method for expressing risk exposure from interconnected digital environments to the organization in business terms [Gartner; Cyber Risk Quantification: Hype Cycle for Risk Management, 2020 (G00442047)]

The mathematical models leveraged to measure cyber risks include the Bayesian Network, FAIR, CVaR (Cyber Value at Risk), Hubbard, and Seiersen (H&S) among others.

(Threat + Vulnerability + Impact) x (Probability + Velocity) = Risk

Breach-likelihood and risk quantification in healthcare cybersecurity

According to the HSS, Quantitative methods of risk assessment have the following advantages:

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

Risks to using qualitative measures:

- Subjective
- Lack transparancy
- Lack reproducibility
- Getting reversed risk rankings
- Uninformative ratins
- Zera value of information (VOI)

Leveraging a quantitative approach:

- Transparent
- Repeatable
- Scalable
- Reproducible

[Source: Cox, L. Djangir Babayev, William Huber. (June 9, 2005). 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.

Freund, J. (June 19, 2019).

And, "Gartner 2019 Debate: Quantitative vs. Qualitative Cyber Risk Analysis." Gartner: https://www.risklens.com/blog/gartner-2019-debatequantitative-vs-qualitative-cyber-risk-analysis/]

Why should cyber risk be measured?

The current enterprise risk models followed by the healthcare sector are compliance-heavy. The models followed in this sector include NIST CSF, NACD, and COSO, to name a few.

Currently, healthcare organizations are stringently following all compliances and government requirements, but what is missing is:

1. A cybersecurity strategy that harmonizes enterprise goals
2. A complete picture of all cybersecurity practices, policies, and products in a de-jargonized and un-siloed, integrated manner
3. A culture of cybersecurity that permeates across departments

The philosophy of breach-likelihood prediction is recognized by authorities yet not adopted by organizations - in May 2020, the U.S. Department of Health and Human Services released a report that describes cyber risk management approaches and risk calculation methodologies that healthcare organizations can apply with special guidance for smaller organizations.

Traditionally, qualitative measurements have been used by security leaders to prioritize cyber risks. However, there is no metric to evaluate outcomes. For instance:

- What is the total risk an organization faces after/ despite investing in multiple products and services?
- What is the difference of impact between the riskiest and the second most risky vulnerabilities present?
- Is the difference between cyber risks ranked #1 and #2 the same as that of #2 and #3?
- On what basis is a risk categorized as high/ medium/low?
- What is the efficiency of the cybersecurity products/ services or patching vulnerabilities; if resources are applied to a particular risk, what is the change in the overall risk posture and its RoI?

Breach likelihood scores help healthcare organizations with:

1. Risk Prioritization

- The knowledge of breach-likelihood scores can help enterprises understand their exposure and its real-time impact.
- Based on this data, they can make decisions either to accept the risk yet improve their risk posture by purchasing cyber insurances, accept the risk and forgo any changes, especially when the investment required to mitigate the risk is larger than its dollar value impact, or mitigate the vulnerabilities by defining their cyber risk appetite and cyber risk tolerance.

2. Effective Utilization of Security Resources and Security Budgeting:

- Businesses are 'project' led when it comes to cybersecurity investments. Most of the purchases are to detect threats in the environment, and these services might overlap in their capabilities.
- With breach-likelihood and Digital Business Risk Quantification, organizations can make data-driven real-time decisions such as where to invest and how much investment is sufficient. Effective utilization of limited cybersecurity budget limits duplication of technical abilities and guides investments based on cyber risk priorities.

3. Cyber Resilience

- Quantification of cyber risks enables the Board to make an informed decision about Cyber Insurance premium purchases.
- The information about the real-time enterprise-wide dollar value impact of risk provides an objective metric for cyber risk indemnification.

4. Communicating cybersecurity to the Management, Board, and Key Stakeholders

- According to guidelines, the CEO can be held directly liable for breaches (according to the GDPR). This makes it essential to carry out effective communication to enhance trust from the Board and EC on the cybersecurity team. In addition, a clearer cyber risk understanding facilitates the integration of cyber risk management with enterprise risk management. This makes it more likely for cybersecurity budgets to be increased, based on the Board's understanding of the financial impact of a data breach.
- Stepping away from abstract concepts based on FUD (Fear, Uncertainty, and Doubt), standardizing cybersecurity in terms of a breach-likelihood score that represents the financial impact of a breach is one of the simplest ways to communicate the cyber risks in business terms.

5. Competitive Advantage:

- Every vector of an enterprise - people (employees and patients), policies, processes, technologies, third-party suppliers, and cybersecurity products/ services - impacts the likelihood of a breach.
- The objective representation of the real-time impact of each element in terms of breach likelihood helps in effective cybersecurity strategies and appropriate resource allocation.

SAFE – a unique method to measure an organization's digital business risk.

SAFE - Security Assessment Framework for Enterprise - is a game-changer in the "Cybersecurity and Digital Business Risk Quantification" (CRQ) space. The Supervised Machine Learning engine of SAFE gives an output both in the form of a Breach Likelihood Score (between 0-5) and the dollar value risk the organization faces, along with providing prioritized actionable insights based on technical cybersecurity signals, external threat intelligence, and business context of what and where are the "weakest links" across people, process and technology. This will enable an organization to measure and mitigate its cyber risk in real-time.

SAFE allows an organization to get an Enterprise-Wide, Objective, Consistent & Real-Time Visibility of its overall Cyber Risk Posture that can be decomposed into five vectors:

1. People Assessment (via SAFE Me)

A zero-permission mobile application to be downloaded by every employee of the organization that helps them assess their cybersecurity awareness, protect their mobile devices (by monitoring cybersecurity controls of their phones), and monitor their deep and dark web exposures. It allows the organization to run cybersecurity awareness campaigns from a library of over a hundred multi-language nano (3-minute) cybersecurity courses and quiz along with monitoring daily of the employee's personal information/password that is leaked to the deep and dark web and put this together in our Scoring Engine to give a score per employee.

2. Process / Policies Assessment

Based on inputs of each cybersecurity policy deployed across an enterprise, a score is generated per policy. There is a repository of 25+ compliances, over 40 cybersecurity policies, and 4400+ process-level controls. These policies are mapped to popular compliance frameworks such as NIST CSF, NIST SP 800-53, PCI DSS 3.2, ISO 27001, among others.

3. Technology

Daily Security Configuration (Hardening) Controls Scanning of every IP Address and taking API feeds of vulnerability scanners in the IT/Cloud Network of the organization and its data ingested into our scoring engine to give output as a score per IP address / Application or Cloud Instance. SAFE applies a patented Bayesian Network-based supervised Machine Learning algorithm to assign a score between 0 to 5 to every asset - a normalized view to provide an objective understanding, aligned with the breach likelihood of your organization through the asset.

4. Third-party

Through SAFE - X, enterprises receive a real-time 360-degree Endpoint, People, and SaaS-based cyber risk assessment of all third-party vendors in the business network. This eliminates blind spots arising from point-in-time assessments that rely on 'trusting' the vendor to be truthful about their cybersecurity practices. It also assesses all vendors, not just the largest or top 10-15% of the riskiest vendors. It also enables you to contextualize and prioritize the risk information collected to strategically allocate and mitigate cyber risks. This allows truly data-driven prioritization of cyber risks through information regarding third-party breach-likelihood.

5. Cybersecurity Products

Score per cybersecurity product on how they are implemented within the network. Some of it (e.g., NGFW, EDR, SIEM) will be based on API feeds, while other categories of products will be objective questionnaire-based.

SAFE Scoring Model:

The SAFE scoring model has been built as joint research at Massachusetts Institute of Technology (MIT) that incorporates cybersecurity sensors data, external threat intelligence, and business context and places it together in a Bayesian Network of a Supervised Machine Learning risk quantification engine to give out scores and dollar value risk that the organization is facing. The scores are calculated at a macro and micro level and can also be measured for particular Lines of Business (LoB) / Crown Jewels / Departments. The SAFE score output is essentially a function of how likely an enterprise will get breached in the next twelve months based on their real-time cyber risk posture.

Conclusion

By adopting a quantitative risk-based cybersecurity strategy, healthcare organizations are more equipped to direct investments, identify and address critical skills gaps, evaluate the efficiency and effectiveness of control frameworks and suggest business justifications for security investments. By objectively measuring the risks, the Board and security teams can truly appreciate the dollar value impact of data breaches. More fundamentally, chief information security officers and chief information officers can provide their internal and external stakeholders with data-driven answers around how secure they are today.

1. A predictive analysis of your enterprise's breach likelihood
2. Prioritized actionable insights based on your current cyber risk posture
3. Objective assessment of the cyber risk posture of electronic Medical systems, Medical Devices, Departments, hospital/ clinic branches, patient data, and more
4. Consistent monitoring and assessment of internal and external technology and cybersecurity Products
5. Real-time quantification of risk posed by your employees/ vendors across the devices they use, deep & dark web, their cyber consciousness, amongst others

SAFE
SECURITY

www.safe.security | info@safe.security

3000 El Camino Real,
Building 4, Suite 200,
Palo Alto, CA - 94306