Code DARK: Leveraging the Human Firewall

Simmy King, DNP, MS, MBA, RN-BC, NE-BC, CHSE, FAAN, and
Andrea Kraus, CCAP

Health care organizations can no longer afford to "bolt on" cybersecurity elements to projects and initiatives in an ad hoc style. To best prepare our health care system to address cyber risks, it's important to consider both the technical and human aspects of a robust cybersecurity program. Cybersecurity works best when it employs a "layered defense"—multiple layers of security built into the organizational infrastructure that provide additional coverage should a threat bypass a single layer of protection. Code DARK is a user-centered strategy that leverages the human firewall, empowering our first responders to be active participants in our cyber defense efforts.

THE EVOLVING ENVIRONMENT

Our health care ecosystems are constantly evolving, and digital health care is an intrinsic component of that ecosystem. As health care providers, we are entrusted with the highest standards of care delivery, and quality, and we are also required to protect the privacy and confidentiality of our patients' data. Managing cyber threats and mitigating cyberattacks across any health care organization comprises complex and challenging tasks. Health care organizations have been and must continue to employ effective cybersecurity strategies to prevent, minimize, mitigate, and address these cyber risks, threats, and attacks—and that includes being as prepared as possible for new and emerging threats. As the digital footprint in health care grows, we must be vigilant and adapt to these increased digital risks. Health care organizations can no longer afford to "bolt on" cybersecurity elements to projects and initiatives in an ad hoc style. Cybersecurity and cyber-hygiene must be built into projects and initiatives from the planning phase, and ensure it is interwoven throughout the organizational ecosystem.

To best prepare our health care systems for cyber risks, it's important to consider both the technical and human aspects of a robust cybersecurity program. Cybersecurity works best when it employs a "layered defense"—multiple layers of security built into the organizational infrastructure that provide additional coverage should a threat bypass a single layer of protection. Inherent to building such a layered defense should be the realistic understanding that there are significant challenges in building and maintaining a holistic cybersecurity program.

One of the most daunting headwinds in tackling cyber threats is the cyber workforce gap. Our cybersecurity and information technology (IT) professionals are an intrinsic support component of our patient care teams, and an inadequate cyber workforce means there may not be enough skilled personnel available to provide the support needed to protect an organization's environment. According to a 2021 report by International Information System Security Certification Consortium, or (ISC)$^{2®}$, the world's largest nonprofit association of certified cyber professionals, there is an extreme shortage of cybersecurity professionals, and the global cybersecurity workforce needs to grow by 65%, or more than 2.7 million workers, in order to effectively defend organizations' critical assets.[1] The United States alone has over 700,000 open cybersecurity positions to fill, and the gap is increasing.[2] This shortage of skilled IT workers necessitates organizations to consider all strategies when developing a cybersecurity organizational mindset, including a first responders approach that engages frontline workers to leverage the human firewall.[3]

KEY POINTS

- **Cyberattacks can and will happen in health care.**
- **Cybersecurity works best when it employs a "layered defense."**
- **A user-centered strategy can leverage the human firewall and empower first responders to be active participants in cyber defense efforts.**

DEFINING CYBERSECURITY AND ITS RELEVANCE

But what is cybersecurity, exactly? It's a topic we hear in meetings, on the news, and among our colleagues,

and oftentimes, health care professionals are unclear about cybersecurity and how it impacts our organizations and work. Cybersecurity has much in common with health care. It is both the art and science of providing quality patient care by being proactive and reactive, albeit to digital threats. Cybersecurity serves to protect networks, devices, and data from unauthorized access or criminal use through technology, tools, and human vigilance.[4] There are protocols and best practices guided by evidence that constitute proper cyber-hygiene—practices such as strong password management, phishing awareness, and even protection against physical threats are vital to a "clean" cyber environment.

Cybersecurity professionals not only strive to protect networks from intrusion, but they also investigate and collect evidence during and after malicious events, with the intention to mitigate an active incident and apply lessons learned to potential future incidents. All of this is meant to ensure the confidentiality, integrity, and availability of information. In other words, cybersecurity helps to ensure that our data are protected against unauthorized access, not tampered with, and that we can retrieve that data promptly. Although health care organizations have historically lagged behind other business industries, the past decade has seen an increased understanding of cyberattacks and their impacts, and most health care organizations have devoted significant resources to hardening their networks against malicious actors eager to hold organizations hostage.

However, even a well-protected organization is at risk. The question is usually not if, but when or how a cyberattack will manifest. Keeping health care organizations safe is not easy. Like other sensitive data, health care data are complex and difficult to secure. Health care organizations are a particularly valuable target for malicious actors because medical data, particularly PHI (Private Health Information) and PII (Personally Identifiable Identification) can be used for a multitude of illegal activities. Medical data are a high value target to malicious actors due to the number of illicit activities that one medical record can support and the difficulty in altering the information. According to the financial megafirm Experian, medical records can go for up to $1000 on the dark web. Comparatively, credit/debit card numbers cost about $100, and individual drivers licenses can cost $20.[5]

It is particularly vital to protect sensitive information through encryption, both while being transmitted and while being stored, which requires additional specialized training in encryption protocols and proper digital forensic practices. As health care organizations are being assessed for a variety of compliance standards, (HIPAA [Health Insurance Portability and Accountability Ac], HITECH [Health Information Technology for Economic and Clinical Health Act], HITRUST [The Health Information Trust Alliance], ISO [International Organization for Standardization], etc.) organizations must recognize that their cybersecurity posture can have a significant impact on their ability to secure lower cybersecurity insurance premiums.[6]

STRATEGIC APPROACH TO CYBERSECURITY

There is no scenario by which any organization with a presence on the Internet has zero risk. Cybersecurity is built along the premise that a layered defense has a better chance to block and mitigate attacks as they arise. Organizations around the world use frameworks and solutions to protect their networks and data from attacks and disruption. In the United States, the National Institute of Standards and Technology (NIST) developed a cybersecurity framework designed for business industries. NIST's Cybersecurity Framework (CSF) (*Figure 1*) contains guidance based on existing standards and best practices that best align with organizational goals.[7] The framework is not designed to be a one size fits all, instead organizations can develop their cybersecurity strategy guided by the framework and their unique risks.

The 5 main components of the CSF are iterative and loosely defined as:

1. ***Identify.*** To protect your organization, you need to know what that organization possesses, physically and logically. What data do you have and where are the data located? How many computers, servers, and other devices—to include mobile devices—are under your safekeeping? Keeping an updated tally of what you are responsible for is the first step in protecting those assets.
2. ***Protect.*** Once you know what you have, you need to develop and execute a plan on how to protect these assets, often through software solutions, but also via hardware and physical solutions. In addition, devices connected to the network should be protected, for example with antivirus software, to keep malware from easily entering the network environment.
3. ***Detect.*** The organizations' cybersecurity program should monitor their networks and devices connected to those networks to ensure that the devices remain clean, and that any potential malware, unauthorized access, or other anomaly is detected, logged, and addressed as soon as possible.
4. ***Respond.*** An organization should endeavor to remediate problems as soon as possible, to decrease the malware/malicious event's area of damage.
5. ***Recover.*** Once an active attack or incident has been mitigated, an organization needs to document what happened, apply any lessons learned to future incidents, and if necessary, bring the network and computing devices back to full functionality. This is the step where an organization assesses how much

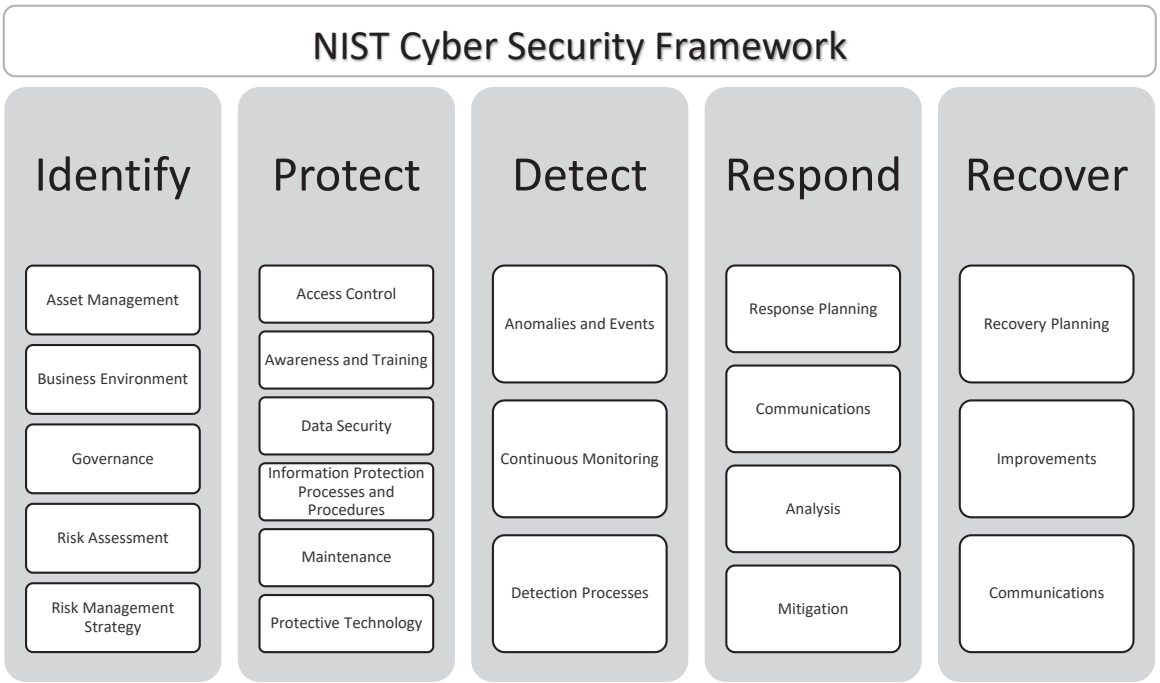

Figure 1. NIST Cybersecurity Framework- Core functions and outcome categories within each function

the incident has cost them, not just in tangible assets, but through often unseen means (reputational cost, lost hours, etc.).

RANSOMWARE—HOLDING DATA HOSTAGE

In the past decade, one of the most common and most dangerous forms of malware is ransomware, and it is leveraged on many businesses and organizations, from civil to private holdings, from government to health care and everything in between. These attacks are considered threat-to-life crimes because they can directly threaten a health care organization's ability to provide patient care, which then puts patient safety at risk.[8] A Sophos whitepaper published in May 2022 reported that 68% of health care organizations were hit by ransomware in the last year, a 30% increase from 2020.[9]

Ransomware is a type of malware that is designed to encrypt files on a computer, and often hops laterally to other computers and servers. It is most often launched as a payload inside of a phishing or spear-phishing e-mail. Once the data are encrypted, the cybercriminals demand a ransom, paid in crypto-currency to protect anonymity to regain access the data or the servers. Sometimes, even if the ransom is paid, organizations will not get full access to their systems, and the hackers often release the data they stole on the dark web or black market websites.

When an organization experiences a ransomware attack, it's not just a matter of fixing the problem and continuing onward. According to *CSO Online* magazine, a ransomware attack can have multiple consequences for an organization.[10] First is the ransom, which could be in the millions of dollars, should the organization decide to pay. Second is the extreme disruption to business and health care operations. If the ransomware disables the network, access to patient records, medical devices, and even communication (telephones, e-mail, etc.) could be unavailable. A ransomware attack can disrupt a health care organization for days, weeks, even months, resulting in disruptions to clinical, administrative, and financial operations. Further, the hidden costs to ransomware attacks that health care organizations may not immediately consider include legal costs, patient and vendor lawsuits, reputational costs, cybersecurity insurance costs, lost revenue, lost data, and more, in addition to considering the amount of time required for cyber professionals to remediate the threat, back up data to the last known good point, and ensure the network is free of malware before resuming business operations.

LEVERAGING THE HUMAN FIREWALL

Simply throwing an army of cybersecurity professionals into your IT department, or indiscriminately investing millions of dollars in high-tech tools isn't enough to mitigate cyberattacks. Regarding cybersecurity, people tend to be the weakest link, and human action can be the root cause of a cyberattack or increased cyber risk.[11] Therefore, all staff must be engaged as part of the organization's human firewall, serving as first

defenders and first responders when facing cyber risks. This is accomplished by creating a security-minded culture, where staff know the importance of the data they safeguard and how they are actively protecting data and infrastructure. The importance of cybersecurity awareness and vigilance cannot be overstated, and all staff, regardless of their role and function, must know how to properly identify, report, and respond to potential threats. By implementing good cyber hygiene practices, staff are empowered to defend and respond—protecting their organization, patients, and data. Cyber hygiene practices that have been employed at our organization include annual cybersecurity, phishing and ransomware education, phishing exercises, cybersecurity governance, and threat management strategies that support are aligned with the NIST Cybersecurity Framework.

CODE DARK

In 2021, Code DARK (*Figures 2 and 3*), a user-centered strategy that recognizes the important role of the frontline staff as a human firewall, was implemented. Code DARK also supported the integration of a cyber response into the hospital's existing culture by aligning with the hospital's established framework and nomenclature for emergency response, such as Code Blue (a hospital-wide notification and response to a patient in cardiac or respiratory arrest).

Code DARK is activated by the IT security leadership when the hospital is actively combatting a cyberattack or experiencing an unplanned, extended downtime that make assets and/or the network unavailable. It is not initiated for routine/scheduled system maintenance or short network disruptions. Code DARK provides staff with specific actions to minimize the damage—the "blast radius"—of a ransomware attack, by systematically and safely disconnecting computers from the locus of infection. This coordinated response and set of actions across the hospital is also aimed to minimize impact and support the continuity of business operations. Education and training occur at all levels of the organization, beginning with new hire onboarding, where all new hires receive the Code DARK badge, and through presentations, intranet resources, and in-person rounding.

Code DARK is an easy-to-follow protocol that can be used during a cyber emergency. It provides staff with simple instructions on how to respond to the immediate concern and minimize any impact/disruption in workflows and patient care.

- ***D****ISCONNECT* workstation(s) and Internet connected device(s).
  - Staff are educated on how to identify what an asset is and how to disconnect it safely—preferably by not turning the asset off. Our training modules explain how to safely remove Ethernet and Wi-Fi devices connected from the network, and what to look for. We also provide guidance on what *not* to unplug due to safety or health concerns. By disconnecting nonessential assets from the network, we can limit the number of devices that could be potentially infected without compromising the integrity of the data on each device.
- ***A****WAIT* instructions from your IT department before reconnecting computers.
  - Like an infection, we want to ensure that as few computers are affected as possible. In the case of malware, it must be scrubbed off the network before "clean" computers can be reattached, or else the infections can reoccur. This step also reassures our staff that our IT security and IT operations staff are addressing the incident and will provide further instructions and information. Communications is key, and status briefings are essential to keep all staff aware of the situation.

Figure 2. Code DARK Badge Card (front) Children's National Hospital, 2020©

Figure 3. Code DARK Badge Card (back) Children's National Hospital, 2020©

- ***R****EPORT* to your managers for department-specific downtime actions.
  - This step further enforces good communication within teams. In the event of a Code DARK when the network must be taken down, unavailable resources could include VOIP (Voice Over IP) phones as well as e-mail, Internet connectivity, Wi-Fi, and even cellular connectivity. We want our staff to treat Code DARK as they would any other code called in an emergency and work with their leadership to continue patient care as seamlessly as possible without these digital resources.
- ***K****NOW* and follow your department's emergency policies and procedures.
  - Each department has a set of operations and procedures for operating without the use of electronic equipment. This step reminds staff that they should be familiar with their role in the event of an emergency. IT security would be working hand in glove with the organization's marketing and communications team as well as the emergency management team to ensure that we are all adhering to business continuity plans and minimizing operational disruptions.

Code DARK is designed to mitigate the impact of ransomware attacks similarly to how health care organizations approach infection control. By employing good cyber hygiene, we can minimize infection and the damage that infection can do. Like all emergency response plans, we hope we will never have to activate Code DARK. However, systemizing this code allows us to drive our security-minded culture. Deploying and incorporating Code DARK in our environment supports our education and readiness strategy by providing staff with an accessible tool that outlines their cyber response to a cyberattack.

In addition to Code DARK education, we use a multipronged strategy to ensure that staff training also includes general IT security. Annual and periodic IT security training are required, and we distribute information regarding general IT security practices and reminders through multiple channels—including situational briefs, meetings, and a robust internal website with resources. In addition to formal training, we employ job aids, tips and tricks, and personnel available for staff to engage with questions. All of this provides a high touch method to keep cybersecurity front and center in the minds of our staff—and to ensure that all staff are operating in a cyber-hygienic mode.

CONCLUSION

Cyberattacks can and will happen in any business environment, especially in health care. Malware, including ransomware, is disrupting business operations and patient care, and can cost health care organizations hundreds of millions of dollars each year in overt and hidden costs. Developing a security mindedness culture can help reduce the risks and potential damages. Code DARK is a user-centered strategy that leverages the human firewall, empowering our first responders to be active participants in our cyber defense efforts.

REFERENCES

1. (ICS)$^{2®}$. 2021 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. Accessed October 5, 2022.
2. Cyber Seek. Cybersecurity Supply/Demand Heat Map. Available at: https://www.cyberseek.org/heatmap.html. Accessed October 5, 2022.
3. The Joint Commission. New Quick Safety Advisory on Building a Culture of Cybersecurity. 2021. Available at: https://www.jointcommission.org/resources/news-and-multimedia/news/2021/10/new-quick-safety-advisory-on-building-a-culture-of-cybersecurity/. Accessed October 4, 2022.

4. Cybersecurity & Infrastructure Security Agency (CISA). Security Tip (ST04-001): What Is Cybersecurity? 2019. Available at: https://www.cisa.gov/uscert/ncas/tips/ST04-001. Accessed September 9, 2022.
5. Stack B. Here's How Much Your Personal Information Is Selling for on the Dark Web. Available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. Accessed October 4, 2022.
6. HITRUST Alliance Inc. Healthcare Sector Cybersecurity Framework Implementation Guide. 2016. Available at: https://www.cisa.gov/sites/default/files/publications/HPH_Framework_Implementation_Guidance.pdf. Accessed October 14, 2022.
7. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2018. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed September 9, 2022.
8. Riggi J. Ransomware Attacks on Hospitals Have Changed. Available at: https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed#:~:text=Ransomware%20attacks%20on%20hospitals%20are%20not%20white%20collar,patient%20care%2C%20which%20puts%20patient%20safety%20at%20risk. Accessed October 4, 2022.
9. Sophos. The State of Ransomware in Healthcare 2022. 2022. Available at: https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf. Accessed October 19, 2022.
10. Brumfield C. SEC Filings show hidden ransomware costs and losses. Available at: https://www.csoonline.com/article/3654293/sec-filings-show-hidden-ransomware-costs-and-losses.html. Accessed October 4, 2022.
11. Kim L. Cybersecurity awareness: protecting data and patients. *Nurs Manage*. 2017;48(4):16-19.

Simmy King, DNP, MS, MBA, RN-BC, NE-BC, CHSE, FAAN, is chief nursing informatics and education officer, Andrea Kraus, CCAP, is manager, Cybersecurity Awareness, Training & Exercise, at Children's National Hospital in Washington DC. Dr. King can be reached at simmy.king@childrensnational.org.

Note: The authors declare no conflicts of interest. The authors did not receive any specific grant from funding agencies in public, commercial, or not-for-profit sectors.

1541-4612/2023/$ See front matter

https://doi.org/10.1016/j.mnl.2022.10.012