Hacking and other types of computer intrusions are increasingly sophisticated. Healthcare organizations have to quickly assess what is happening and defend their organizations and data from these incidents. A robust cybersecurity solution leverages people, processes and technology – working in concert – to defend and protect the healthcare organization’s most valuable asset: information.
People: All Hands on Deck to Protect and Defend

According to the 2015 HIMSS Cybersecurity Survey\(^1\), nearly two-thirds of respondents indicated that a lack of appropriate cybersecurity personnel was a barrier to mitigating security incidents. Additionally, cybersecurity personnel play a key role in managing risk at an organization. Some organizations may have sufficient expertise in-house and thus may not need to outsource, except in unusual or exceptional situations (e.g., a sophisticated cyber attack resulting in a massive breach). Other organizations, however, may lack sufficient numbers of cybersecurity personnel or may lack cybersecurity personnel who can perform certain tasks or functions (e.g., penetration testing). Whether it is a lack of personnel or expertise, many healthcare organizations find outsourcing solutions to fulfill these needs.

What’s more, these solutions are tailored to meet each organization’s unique needs. For example, Cisco Advisory teams assist wherever an organization may be in its security journey. This might include developing effective security and compliance strategies, or creating a programmatic approach to securing mobile, cloud and digital environments.

A key benefit of supplementing an internal team with external experts is the objective perspective and cutting-edge technical training these professionals offer. OnX Enterprise Solutions, a global technology integrator with a staff of highly certified security solution principals, provides assessments that recommend unbiased, collaborative cybersecurity solutions incorporating best-in-class original equipment manufacturers and independent software vendors. In addition, OnX provides chief information security officer services with an eye towards HIPAA/HITECH compliance and risk management. These include guidance on building a governance board, service level agreement review, education and training.

Staying ahead of cyber risks is an ever-changing, full-time job that can be a challenge for any organization. Combining inside and outside perspectives gives healthcare organizations a holistic view of their cybersecurity risks to better protect and defend their information from unauthorized users and entities.

Processes: Cybersecurity in Action

Processes are the glue that binds the people to the technology in cybersecurity. If the appropriate processes are not in place, significantly adverse consequences can result. In fact, a lack of appropriate processes can lead to a haphazard and inconsistent approach to assessing and managing risks. In turn, a healthcare organization’s defenses may be weak because of many unaddressed vulnerabilities.

Processes need to be finely tuned to an organization’s needs and requirements by being part of a written plan. The plan serves as a blueprint for the organization’s cybersecurity program, and should be tested and validated regularly. It outlines what gets done, when and how – and, specifically, who the players are, what the processes are, what technology is used and how it is used. The plan also includes contingencies to address a manmade or natural disaster, such as a hacking incident or a hurricane. Further, the plan is a living and breathing document that changes with shifts in personnel, processes and new or different technology.

Whether healthcare organizations need to build or improve upon their security plans, OnX Enterprise Solutions helps them adopt and implement security frameworks and establish best practices. It also can review and provide expert input on an organization’s processes, with an eye towards helping secure the entire health IT ecosystem. This includes considerations for mobile medical devices, electronic health records and the data within. OnX also helps healthcare organizations improve their processes to defend their large and/or fragmented networks against pervasive and highly sophisticated attacks.

Cisco Advisory teams assist healthcare organizations with their plans to identify, detect, protect, respond or recover from security incidents. Tapping this expertise, enables healthcare organizations to establish appropriate cybersecurity processes to protect and defend their information.

Planning, preparation and testing of ongoing cybersecurity processes provides a critical defense against threats to patient and healthcare information. In the event of a minor or catastrophic attack, finely tuned processes also ensure healthcare organizations are able to successfully respond to contain the damage and return to operations.

Technology: Tools to Identify, Detect, Protect, Respond and Recover from Security Incidents

The mainstays of many healthcare organizations’ cybersecurity technological solutions, including firewalls and anti-virus software, have been around for many decades. Meanwhile, the threat actors have become quite sophisticated and their tactics quite advanced. In the face of this new reality, healthcare organizations must evolve their technology solutions to include and, indeed, embrace more advanced solutions. For example, intrusion prevention systems, data loss prevention solutions, security information and event management systems are robust solutions organizations need today. These tools help secure the information technology environment at all stages: identifying, detecting, protecting, responding and recovering from security incidents.

To this end, OnX recommends and implements the appropriate state-of-the-art cybersecurity products and services that align with an organization’s objectives. For example, mobile technology and bring your own device (BYOD) programs add value, but also could add risk. OnX helps organizations stay abreast of mobile technology and trends to implement or enhance BYOD programs that reap the benefits without compromising security.

Hyland’s OnBase Information Management system is architected so that multiple barriers to cyber-attacks can be prevented. The system configured to meet and exceed the most stringent of security policies, including ensuring all the information it manages is strongly encrypted. Moreover, the OnBase system ensures that only the right people have access to the right data at the right time and under the right circumstances.

Malware is constantly evolving and can be relatively difficult to detect – stealth malware is becoming increasingly common. Leveraging the power of big data analytics, Cisco security solutions can determine if a file is actually
malware – even if it is considered to be good by most traditional security solutions. Upon detection of new malware, an organization’s staff are alerted and the scope of compromise is identified. This includes information on how the malware spread through the network environment, whether any personally identifiable information or protected health information has been compromised, among other topics. Detecting malware is one thing; stopping the spread is another. And, Cisco security solutions are capable of automatically stopping the malware from spreading and remediating it without needing human intervention. Such automatic solutions are essential to help close the gap between the time a breach occurs and when it can be remediated.

Cisco’s technological solution provides visibility and performs analysis of the users and devices connecting to a healthcare organization’s network. Cisco Identity Services Engine (ISE) unifies and automates secure access control for networks and resources, both wired and wireless. It features advanced identification technologies that create contextual identities such as user, device or location. Policies are administered at the point of access, which enforces and validates security compliance.

Further, Cisco’s “Network as a Sensor and Network as an Enforcer” solutions work together to provide an organization with deep visibility into its network. This lets healthcare organizations know exactly who and what is on the network at all times, thereby establishing a reliable baseline with regard to what the traffic flows look like (e.g., applications, users and devices that are known, as well as unknown across the network). Leveraging this information, the organization can determine if there is anomalous or suspicious behavior that requires action.

Additionally, Cisco security solutions span the continuum of attack scenarios: before, during and after.

• Before an attack: Profile the network to understand what needs defending – the who, what, where, when and how. This is being visibility driven. It is essential to accurately see what’s really happening in the environment to understand what is typical and what constitutes a threat. Visibility needs to come from the network fabric, endpoints, mobile devices, virtual environments and the cloud. The more organizations see in their networks, the more they can correlate this information and apply intelligence to understand context, make better decisions and take action – manually or automatically.

• During the attack: When attacks do get through, detecting them, understanding them, blocking them and defending the environment against them is the priority. Policies and controls are important to reduce the surface area of attack. In this environment of advanced malware and zero day attacks, it is an on-going process that requires continuous analysis and real-time security intelligence, delivered from the cloud and shared across all products for improved efficacy.

• After the attack: Invariably attacks will be successful. In such instances, healthcare organizations need to be able to determine the scope of the damage, contain the event, remediate and bring operations back to normal. Continuous network monitoring and analysis are gold standard security solutions to record, understand and apply what is being “seen” in the network.

Threats to patient and healthcare information change rapidly. Healthcare organizations must remain vigilant and rely on state-of-the-art technological solutions to better protect, detect and defend their information from unauthorized users and entities.
Conclusion – How to Get From Here to There

Cybersecurity is a rapidly growing and dynamically changing field. It appears to be a maze. And, while not while not an easy endeavor, it can be manageable with the right people, processes and technology – and with help and assistance from experts, when needed.

Healthcare organizations must now quickly grow their capabilities in cybersecurity, especially given the sharp rise in cyber attacks in recent years. All organizations need to agilely adapt to this new terrain; no one is immune to compromise. The risk to safety, security and trust are too great. The healthcare community must continuously learn and collaborate with one another to become more resilient for the industry as a whole and to protect patients, the ultimate benefactors. In so doing, the Global Center for Health Innovation will be the spark for collaboration, learning and discovery along the healthcare cybersecurity journey.

Contributing Tenant Partners

- **Cisco** – Cisco provides expertise to design and implement security solutions and can help validate, implement and migrate to new technologies securely while working closely with your organization. More at: [www.cisco.com](http://www.cisco.com)

- **HIMSS** – HIMSS provides resources to assist healthcare organizations and business associates with their privacy and security initiatives. More at: [www.himss.org](http://www.himss.org)

- **Hyland Software** – Hyland’s Enterprise Information Management System, is architected and programed so that all of the information it manages is secure and makes it easy for healthcare organizations personnel to configure highly secure systems. More at: [www.onbase.com](http://www.onbase.com)

- **OnX Enterprise Solutions** – OnX Enterprise Solutions, a global technology integrator, with its highly certified staff of security solution principals provides assessments that recommend unbiased, collaborative cybersecurity solutions incorporating best-in-class OEMs and ISVs. More at: [www.onx.com](http://www.onx.com)