Microsoft

DIGITAL TRANSFORMATION IN HEALTH

Vigilant

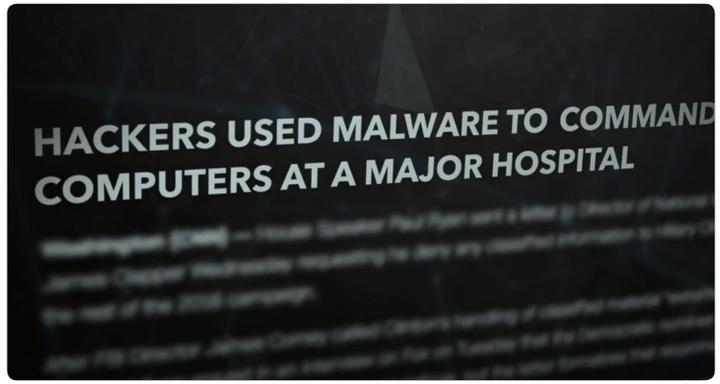
CYBERSECURITY

Table of contents

Unauthorized disclosure. Theft of patient records. Ransomware. Cybersecurity in health is at the top of the news, and it's top of mind for every health provider, payer, regulator, and patient.

Too many organizations don't realize how sophisticated cyberattacks have become. Hackers are no longer mischievous high school kids hiding in their parents' basements. They are well organized, with tools in their arsenals that include easily obtainable software development kits—complete with product support. Yet, based on security reports from Kaspersky, Experian, Verizon, Mandiant, and others, organizations remain remarkably vulnerable.

Cybercriminals find their way in through unpatched and unsupported (old and out-of-date) systems, weaknesses in apps or devices, and carefully orchestrated social engineering attacks. They exploit any new security hole within moments of its discovery, sometimes within minutes. They are a determined group, well-funded by criminal syndicates and even nation states. Countering these forces is a never-ending, continually escalating race.



"When we talk to health organizations about security, we find there is a huge education curve," said Raj Gupta, Chief Technology Officer of Lumen21, which helps organizations achieve and maintain compliance. "Eighty to ninety percent of them focus on their infrastructure on the back-end side. They assume that if they secure their back end, that is really most of what they need to do. They don't understand the entire surface area of attack."

Richard Turner, Cloud Product Marketing Manager at Barracuda Networks, which offers security products and services, agrees that security can present a steep curve to organizations. "Healthcare organizations know they have to protect their data, and they know that it is up to them to do it," he said. "They're sometimes surprised by the lengths they need to go to, and they're definitely stressed by the amount of management they think security is going to take."

> "[H]ealthcare companies will remain one of the most targeted sectors by attackers, driven by the high value compromised data can command on the black market, along with the continued digitization and sharing of medical records."
> – Experian Third Annual 2016 Data Breach Industry Forecast

Compliance barriers to digital transformation

Few industries face as stringent a regulatory environment as health, and the current conversation about security, privacy, and compliance in healthcare is only getting more complex. Electronic medical records are making patient information more accessible to both care givers and patients, while technologies like mobile devices and data analytics are pushing the boundaries of how organizations think about where to store medical data, how to use it, and who should have access to it.

While advances in health IT are promising, concerns about privacy compliance make health organizations wary of adopting technology solutions they are not absolutely certain they can trust. This is one reason digital transformation in health lags behind other industries. Health organizations must also deal with the quagmire of digitizing mass volumes of highly sensitive data while integrating a wide variety of medical and IT technology that run on completely different platforms—all of which need to be secure and compliant.

Learn about Microsoft's vision for digital transformation in health.

Change your security mindset

In the face of compliance challenges, health organizations may struggle to determine where to begin their digital transformation journey. To cybersecurity experts, however, the starting point is clear. "Digital transformation starts with security," said Hector Rodriguez, Chief Information Security Officer for Microsoft Worldwide Health.

Organizations that treat security like a "bolt-on" to worry about later can land in serious trouble. "Successful customers understand that you need to start with security," said Turner. "The ones who struggle start to deploy their solutions and then find out, mid-way, that they didn't sufficiently plan for security requirements."

According to Ed Don, CEO of Lumen21, security is a black and white exercise. "You don't think it's going to happen to you, that if you are doing what you think is enough and you have a problem, maybe everything will be OK. But I tell people, either you're compliant or you're not. There is no in-between. 'Almost' will not suffice. It's nice to know you are working at being compliant, but if you get caught not being compliant then you're not compliant. You are not going to get credit for effort."

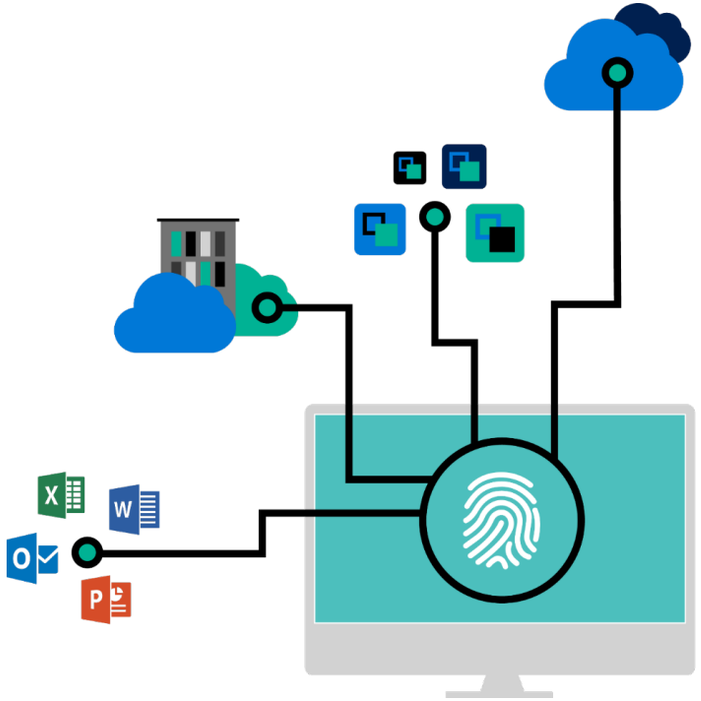
Achieving and maintaining compliance in the age of digital transformation requires a change in mindset. "Not only do you need to think about security first," said Rodriguez, "you need to think about it differently. You have to embed it into your DNA."

"The reality of protecting yourself in this day and age is that it's not inexpensive. It's kind of like when we get car insurance. Nobody wants to get all this goofy stuff to guard against things you think will never happen. But like our Compliance Officer says, 'You never have a problem until you have a problem.'"
– Ed Don, CEO, Lumen21

Assume compromise

Traditional approaches to security focus on keeping the bad guys out. These include deploying firewalls, requiring passwords, and installing anti-malware to protect endpoints like devices or applications. But what if you lock your front door, and someone slips in anyway? "You need to assume that you've already been compromised," said Rodriguez, "because most organizations have. They just may not know it."

In other words, it's not enough to take measures to protect your perimeter. "At Microsoft, we subscribe to the three-sided strategy of 'protect, detect, and respond," said Rodriguez. "The first step is to install stronger doors and locks to keep the bad guys from getting in. But if they succeed, you need to know as soon as possible. This is like putting up cameras to spot criminals as they break into your house. Then you need a way to take swift action, such as locking down a user's account, a lost device, or a stolen document. This is like having home security system that detects motion and automatically turns on all the lights and calls the police."



Make security end-to-end

Security requires a holistic approach across hardware, software, and data for clinical systems, financial systems, administrative systems, productivity tools, and so forth. "This includes systems you use in house, as well as the tools you've given to your mobile workforce," said Rodriguez. Your entire technology stack must be trustworthy. Weakness in any one area can result in a breach that undermines security across all areas.

"Many health organizations assume they are secure because their email or back-end database is secure," said Gupta. "Hackers don't go directly into your back-end systems and extract the database. The vast majority of the breaches we see in large healthcare organizations happen at an endpoint level: from a desktop, from a laptop, or from a user making a mistake."

To combat cybercriminals, organizations have to protect every potential point of entry, which include people, devices, apps, and data.

People are the weakest link

Microsoft research shows that more than 90 percent of security incidents result from human error, not hacks. This includes falling victim to social engineering attacks such as phishing emails and spoofing that allow criminals to steal credentials.

"In the last 18 months ransomware has been a huge issue," said Gupta. "A few of our clients have gotten infected because someone received an email that says 'Hey, you got this package, or you have a bank account that has been locked down, click on this.' The link is actually malicious, and downloads a very small package that you won't even notice because the moment you click on it, it takes you to a legitimate site. Meanwhile, that small package starts proliferating into your internal network, and the ransomware attack begins."

Although health organizations can deploy technologies that help protect against human error, Gupta said, their best weapon is to raise awareness.

Devices are a favorite doorway

Compromising devices like network switches, routers, printers—even medical devices—can give criminals direct access to your network and apps, as well as any data on the device that isn't encrypted. "Even copier machines have physical hard-drives," said Gupta. "Does the vendor who manages your peripheral devices take that into account? If the hard drive from your copier is stolen, your protected health information goes out the door unencrypted. Or maybe someone comes in and replaces your copier hard drive. People don't think that's an important thing, but that's where your breach of information can happen."

Devices include any piece of hardware that runs software. It's critical to keep that software properly patched and maintained.

Beware of apps

Apps, particularly web apps, are an increasingly popular attack vector. "If customers are using development tools to quickly create mobile applications, they have to always be thinking about how they are going to secure them," said Turner.

Vulnerable operations make vulnerable apps even more dangerous. "Technology companies who started out selling applications are now transitioning to the software as a service (SaaS) model," said Don. "We find that some are missing the basics. They may not even have a sense of what policies and procedures they need to have in place to secure their operations. The moment they become SaaS providers of healthcare solutions, they have the same compliance requirements as their healthcare users."

Health organizations need to make sure they talk with vendors about security. Insist on vulnerability testing and validation before deploying any apps into a production environment.

Data loss can be hard to detect

Data is attractive to criminals because they can sell it, use it to impersonate people, or extort victims. "Ransomware is just the flavor du jour," said Turner. "The more insidious issues for healthcare are data theft schemes that include data skimming and data impersonation." In other words, if cybercriminals can gain access to data, they can also tamper with it. "Criminals are realizing that if they can hack hospital data, they can spoof some of that to the insurance company," said Turner. "For example, the ICD-10 codes for atrial defibrillation and a heart murmur are only different by a couple of digits. One condition

requires no treatment. The other is expensive." Hackers try to get in between a patient's records and the insurance company, Turner explained. "They pose as a provider and bill for the more expensive procedure, and because a physician's notes for the two types of conditions look similar, the patient doesn't notice. Her insurance starts paying thousands of dollars to a fake provider for something she doesn't even realize she doesn't have. This is very hard to catch."

The best defense, Turner said, is to build protections around data access. "Insurance companies need to authenticate their providers. They need strict access rules so that when bad actors try this type of scheme, they're blocked."

Create a "defense-in-depth" plan

The best cyber defense is multi-layered. Experts strongly recommend that health organizations create an in-depth security plan comprised of physical measures, technical measures, and operational safeguards.

"When I talk to customers about creating a defense-in-depth plan, I like to quote the old saying 'Trust, but verify,'" said Don. "This is another way of saying, 'I know you told me that you're OK, and that everything seems good, but I'm still going to validate that. This is what we call 'Zero Trust.'"

Learn about the defense-in-depth approach to security, compliance, and privacy of protected health information in Microsoft business cloud services

Physical security measures

In the United States, the leading cause of health breaches since the beginning of 2010 has been theft, which includes theft of paper as well as devices. "It always strikes me when I visit places like doctor groups, clinics, and laboratories that there is a high level of accessibility to patient record information," said Don. "You look past a reception desk and see large, open cabinets that don't have any means to

close them. When everyone leaves and the cleaning people come in, what prevents them from just grabbing a few of those color-coded files?"

Just as you should never leave paper files out in the open, you should never leave servers or devices where people can access them or walk away with them. Microsoft, for example, employs multiple layers to prevent physical access to its datacenters, including perimeter fencing, video cameras, security personnel, secure entrances with multi-factor biometric and token scanners, as well as a sophisticated communications networks.

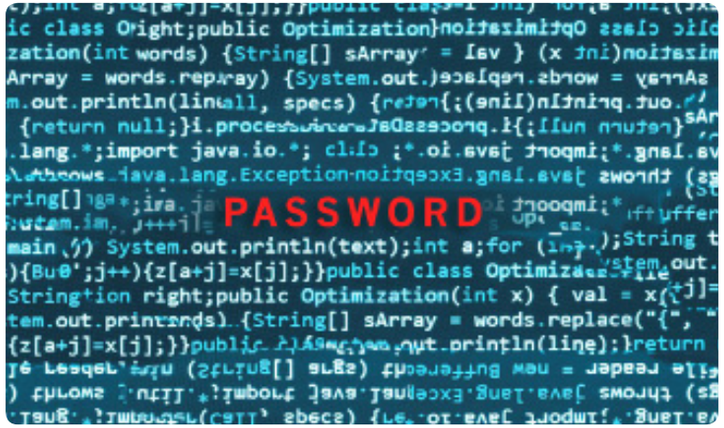
Take a virtual tour to learn how Microsoft secures its data centers.

Technical security measures

The next layers of defense involve technology to help protect end points that may be vulnerable to attack.

Secure your network

Securing your network includes advanced firewalls, packet inspection, antimalware programs, and spam filters. Turner also recommends that organizations isolate their networks. "That's the wonderful thing about the cloud," he said. "It's not a single net. It's multiple nets. You can have different applications on different subnets. You can set up a security hierarchy where not everything runs through one point. There's



not just one door in. You can say who's allowed to go in door one or door two. People used to think of subnets as just a way to load balance. Now it's a way to provide security."

Secure identities and access

Most cybercriminal schemes succeed because of poor authentication controls around people, machines, software, and data. It's therefore important to implement more resilient methods of verifying that people attempting to gain access are who they say they are. With an identity and access management solution such as Microsoft Active Directory or Azure Active Directory, IT departments can set up granular controls that grant secure access to corporate resources and data, including apps, based on an individual's role (nurse) or membership in a group (finance team).

"One of the simplest ways you can address a whole bunch of issues is dual factor authentication," said Don. "We put that ATM card in, it reads the strip, and it asks you to put some other data in, right? There's two factors right there." Don cautions that some people may resist multifactor authentication, because it is an extra step. "When you analyze it, though, that extra step takes all of five seconds. So you have to force a certain discipline, even if it's uncomfortable."

Secure your mobile environment

Mobile device management (MDM) and mobile app management (MAM) solutions, such as Microsoft Intune, help ensure that devices connecting to your network have the latest software updates, as well as the right security configurations, policies, and approved apps. This is particularly important for personal devices people might use to access resources. While managing phones, tablets, and laptops is critical, it's also important to pay attention to the increasing number of IoT devices. "We tell customers to never directly connect devices to the Internet." said Turner. "Some devices use very simple protocols that are easily hacked. We recommend connecting them to a protected subnet first."

Learn how to protect identities, devices, apps, data, and documents with Microsoft Enterprise Mobility + Security (EMS).

Secure your apps

If your organization uses SaaS apps, a cloud access security broker (CASB) solution such as Microsoft Cloud App Security can help you create policies that govern data sharing methods such as storing files in cloud drives or sending them as email attachments. In addition to protecting networks, advanced firewalls can also help protect apps. "Say someone tries to plant a virus in a patient portal," said Turner. "Barracuda's Web Application Firewall can stand in front of that transaction. If something looks suspicious, like someone is trying to access the website from Eastern Europe when we're dealing with American clients, we can shut that communication off. We block that person from ever connecting to your website."

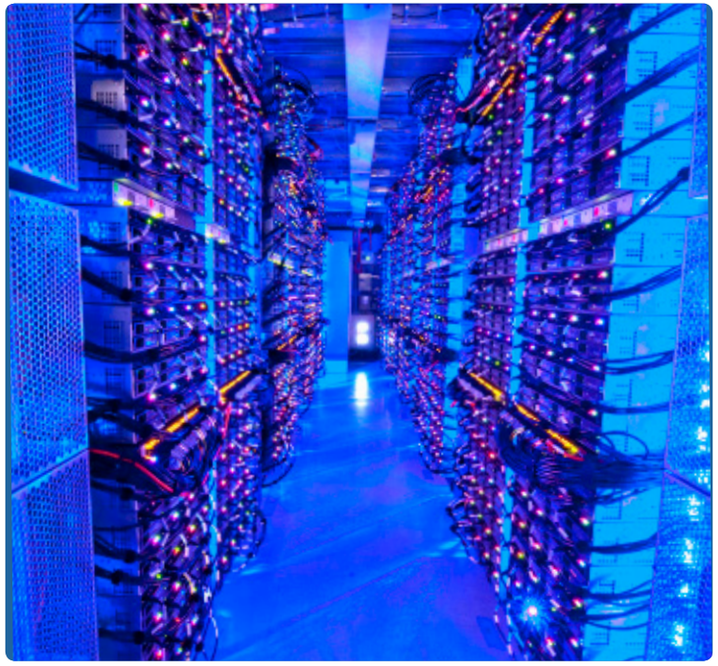
Learn how to protect web applications against application DDoS, SQL Injection, Cross-Site Scripting, and other advanced attacks with Barracuda Web Application Firewall.

If you're developing custom apps, follow secure development practices, such as Microsoft's Security Development Lifecycle, a set of processes and tools that include threat modeling during the design process, code security standards, and tools for testing and verification.

Learn about Microsoft's Security Development Lifecycle.

Secure your data

An essential best practice is to ensure that any data within your network is encrypted on devices and in datacenter storage. Data in-transit should also be protected. "A hack is a two-way operation," said Turner. "This gives us two opportunities to detect and prevent data loss. So our products inspect data on its way in, and on its way out. If we see anything suspicious, like credit card numbers that are heading out the door, we stop the data and alert the administrator. If the data transfer is legitimate, the administrator can override the block. If not, they can contain the problem."



You can also protect data at the document level through encryption and rights management, and by tracking, expiring, and remotely destroying shared documents if necessary. Microsoft Azure Data Protection offers such capabilities. Microsoft also has technology to scan email attachments for common patterns of sensitive data, such as social security numbers, and to prevent operations on documents such as forwarding, copying and pasting, and printing.

Operational security measures

Contrary to popular belief, secure operations isn't just the responsibility cloud vendors. "Office 365 is in a cloud that Microsoft operates securely," said Gupta, "but you are using it locally on your desktops and your mobile devices. You have to secure those too."

"Compliance is not 'one and done.' It's ongoing."
– Raj Gupta, CTO, Lumen21

"Cybersecurity can be hard, because people think 'I have a vendor who's cybersecure, so therefore I am,'" said Rodriguez. "But it's not that easy. You've got to manage it. You've got to know where your data is, and you've got to listen to your signals on an ongoing basis. When it's all said and done, the cybersecurity responsibility matrix includes the cloud services providers, the solution partners, and the end customer."

Microsoft protects customers through both secure development and secure operations practices, going beyond certification requirements with an Operational Security Assurance framework and dedicated cybersecurity teams. Microsoft's approaches are based on decades of experience building enterprise software and running hundreds of thousands of servers in datacenters around the world that deliver more than 200 online services to more than 1 billion customers and 20 million businesses in 88 countries. Microsoft also works with government agencies, industry partners, law enforcement, researchers, customers, investigators, and forensic analysts around the globe to fight against cybercrime. Its dedicated Cyber Defense Operations Center uses sophisticated technologies to visualize, identify and track global cyberthreats in real time, as they develop.

Based on their collective experience operating large datacenters, Microsoft and its partners recommend risk assessments, clear policies and procedures, and awareness campaigns.

Conduct risk assessments on a regular basis

If a healthcare organization is ever breached, it must respond to an audit. "One of the first things auditors are going to ask you to do is show them your latest risk assessment," said Don. "If you say you don't have a risk assessment, that's a bad answer." A risk assessment includes a review of your policies and procedures, both for the technology you have deployed and the people who are using it. Auditors will ask which apps and cloud technology you are using, and whether you have added components to enhance security, such as encryption. They will want to know who your vendors are, and whether you have signed business associate agreements with them that address security.

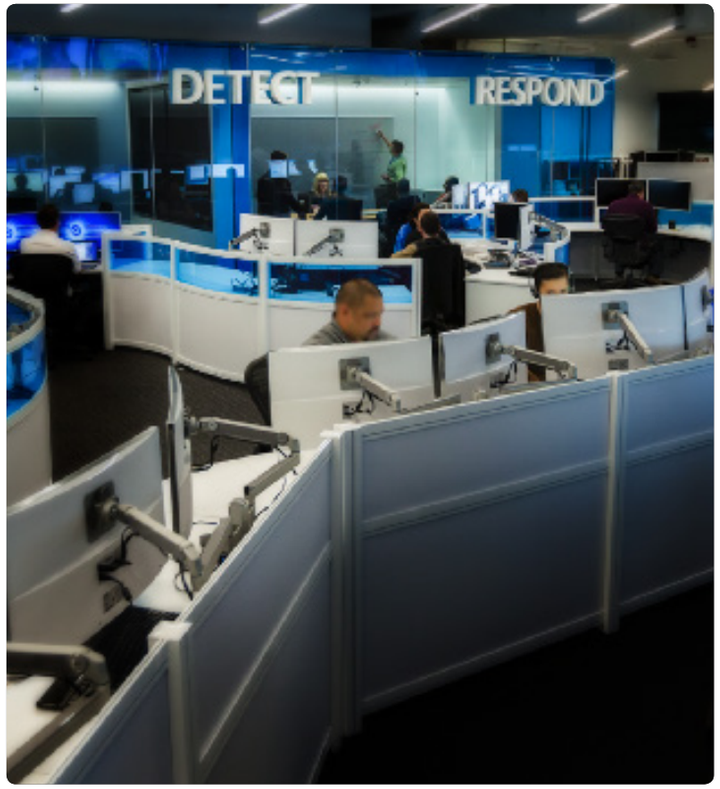
"Customers should continually do risk assessments, because the world is always changing," said Turner. "You should constantly be looking at the vulnerability of your network—every week or every month—because things will change. If you find a vulnerability, you fix it, and then run your tests again to ensure you really fixed it or to see if something else has shown up." Organizations should conduct full risk assessments at least once a year. "Organizations usually find multiple vulnerabilities," said Turner. "Security partners can help them figure out which to fix first."

Define clear policies and procedures

Policies are rules applied via technology. For example, you can require strong passwords that users must change on a set schedule, and use of multifactor authentication. A procedure is how you implement those policies, that is, your method for running day-to-day operations securely. Be sure to document your policies and procedures thoroughly and be ready to share them with auditors. If you have a problem, they can help pinpoint the origin.

Recommended best practices for policies and procedures

- Require use of strong passwords and multifactor authentication. Automatically prompt users to change their passwords every few weeks or months.
- Require PINs to protect all devices that contain data or connect to networks, such as PCs and mobile phones. Use subnets to help isolate devices and apps.
- Configure every user account with "least privileges." Even administrators (and their management chain) should operate as regular users unless they are performing administrative tasks.
- Because hackers use compromised administrator accounts to "escalate privileges" for accounts they use to steal information, keep the number of people with administrative privileges as small as possible.
- Only grant access to apps, document repositories, and administrative tools to users and groups who need it. Frequently audit or review group permissions and memberships to remove people who no longer need access.
- Prevent Shadow IT, such as use of unauthorized SaaS apps, by making it easy for people to find and use the tools they need to do their jobs. For example, create an app portal that users can access via single sign-on.
- Continually monitor your environment and conduct internal audits, so you can quickly identify and address suspicious activity, whether that activity originates from internal or external bad actors.



Raise awareness

Security must be everyone's business, and everyone's responsibility. There's only so much technology can do to prevent people from doing the wrong things. "Your biggest vulnerability is people," said Turner. "It's also the hardest one to address. You can automate technology defenses, but anything people-related really does come down to things like training and personnel risk assessments."

Anyone who deals with data needs to understand the different forms attacks can take, such as phishing and spoofing. They need to understand that habits like reusing their work password for consumer accounts, or transferring work documents via personal cloud storage services, create risk.

Learn how to use PhishPro® from Lumen21 to conduct "friendly phishing" exercises and protect against malicious emails.

One of the most effective ways to raise awareness is a simulated attack that makes the potential consequences of careless behavior readily apparent. During "friendly phishing" exercises, users receive legitimate-looking emails, for example, notices that a package they have been expecting has been delayed. Any user who clicks on a link or attachment in one of these emails receives an alert that they have just succumbed to a simulated cyberattack.

"Mistakes people make can be very simple," said Turner. "I know a guy who once flew a drone inside his company's warehouse so he wouldn't lose it outside. He kicked himself later when it dawned on him that the drone had cameras in it. It's not that people are dumb. They just don't always understand the consequences. They get a new device and plug it in in their office. Now it's on the Internet. Is it secure? Have they even thought about that?"

Get help from security experts

Because the cybersecurity landscape is so complex and changes so rapidly, health organizations benefit from working with partners who specialize in security.

"We hear organizations say that while they are really concerned about security, they prefer to handle the challenges themselves," said Don. "I don't mean to minimize their efforts, but do they really think that two IT pros at a blood clinic are better prepared to handle security and compliance than a Fortune 50 company like Microsoft with all their technology, research, and resources? We work hard to educate these organizations that if they are not in the security business, they probably can't do a better job than a company that is."

"It's important that health organizations have somebody they can turn to on an ongoing basis. There is too much to learn too quickly for them to conquer cybersecurity on their own."
– Richard Turner, product marketing manager, Barracuda Networks

When he encounters a customer who wants to go it alone, Don likes to share a healthcare analogy. "There are specialists in the healthcare industry: brain specialists, heart specialists, liver specialists, and so forth. In our space there are specialists for compliance, IT,

and cloud. You will be well off spending time talking with those specialists. That could help you."

Security in the cloud

Handing off security is enough of a concern to some health organizations that they shy away from cloud solutions. "Somehow the ability to visit their servers in their own data center is more comforting to them than moving them into another facility, the infamous 'cloud' that they can't see or touch," said Don. "I try to point out that if they really want to be secure, outsourcing to a company that has more experience, more expertise, and more safeguards in place is going to be cheaper and better insurance than trying to do it themselves."

"There's a misconception that the cloud is the least secure option," said Rodriguez, "but many health organizations have already started moving to the cloud, because cloud services have achieved a level of scale and security that is very difficult—oftentimes impossible—for them to duplicate and maintain on-premises. If you're not ready to move to the cloud, you have other options. You can implement a private cloud solution. You can transition a step at a time, for example, by starting with a tried and true cloud solution like Office 365."

"The truth is that if an organization isn't on the cloud today, they're probably going to go there," said Turner. "If they're already in cloud, they're probably not there a hundred percent. Companies need to understand what a hybrid network is, and how that impacts security. Hybrid means some of their information and applications will still be protected on-prem. Others will be in the cloud. Where different applications sit might be determined by who's accessing them. Some things are always going to be mobile. Some never will be. This is another area where your partner becomes very important. They can help you set things up the right way."

Monitoring threat signals

Detecting potential and successful intrusions requires sophisticated resources—not just tools, but access to millions of signals plus the advanced algorithms and computing power to monitor them, interpret them, aggregate them, and report them as the attacks are happening. Only a handful of companies have these kind of resources. Microsoft, for example, has data from billions of daily authentications to Microsoft Accounts and Azure Active Directory, as well as telemetry data from hundreds of millions of devices running Windows. Barracuda Networks runs one of the largest 24x7 cybersecurity networks that continuously monitors threat signatures coming in from its products deployed at customer sites worldwide. By monitoring threat signals, companies like Microsoft and Barracuda can take immediate action to contain emerging attacks, for example, by pushing patches out to customers before an attack spreads to multiple geographies. Customers can get help from tools like Microsoft Advanced Threat Analytics (ATA) to automate responses to suspicious activity in their own environments. For example, if ATA recognizes "impossible travel"—someone logging in from Los Angeles and then logging in from China an hour later—it can require a second authentication attempt, with multifactor authentication enabled, before allowing access.

Be Proactive

Victims of ransomware and other successful attacks know well that looking back to assess "what we should have done better" is a painful process. It involves not only expensive fines but damage to reputation and client trust. Although no cyber defense may be absolutely foolproof, every health organization should explore ways to strengthen its security posture by adopting carefully considered security technologies and practices.

Get guidance on preparing for and managing a major cybersecurity incident.

"Don't be afraid of cybersecurity," Turner advised. "The world is out there. You're part of it. Be proactive on how you're being protected. Don't be afraid that you're going to be attacked. Know you are. And plan accordingly."

www.microsoft.com/security