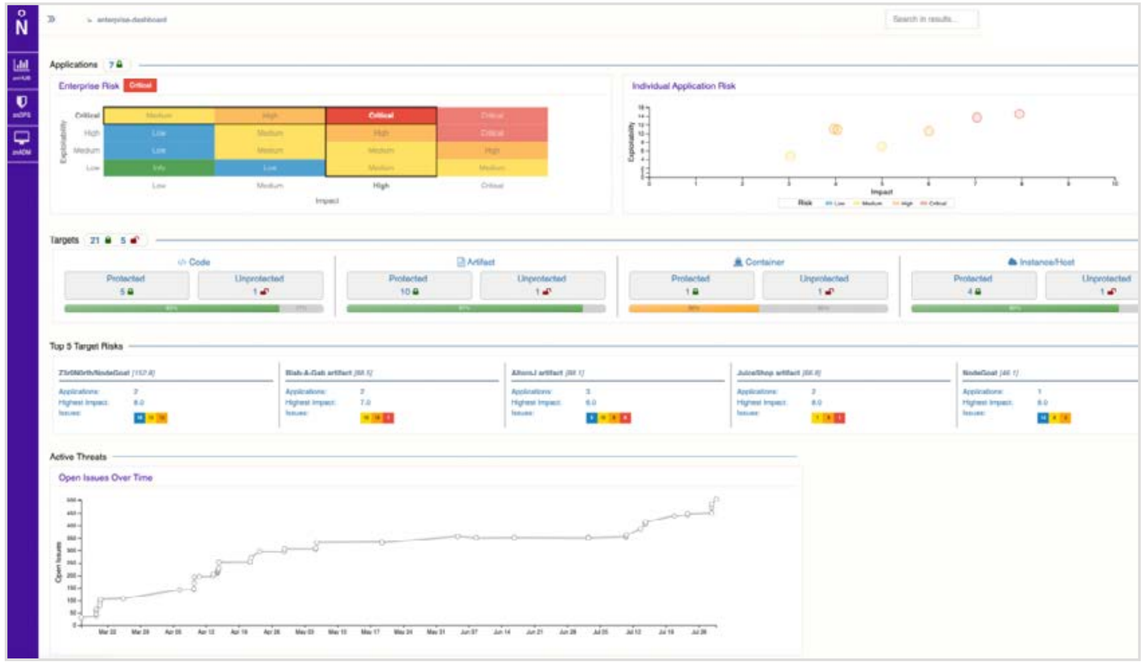
threatpost | Insider eBook

Healthcare Security Woes Balloon in a Covid-Era World

Sponsored by ZERONORTH™



Centrally manage your AppSec program through ZeroNorth to ensure consistent security standards across your organization

ZeroNorth brings security, DevOps and the business together to improve application security performance and reduce organizational risk. The company's application security automation and orchestration platform unites these teams to rapidly identify, prioritize and remove vulnerabilities standing in the way of software excellence. To learn how a large healthcare technology solutions company leverages ZeroNorth to confidently deliver high-quality, secure products to market, see the Case Study on page 24.

Healthcare Security in the COVID-19 Era

In 2020, the healthcare industry began a massive shift, as legacy cybersecurity issues merged with new security challenges spurred on by the spread of COVID-19.

Even before the pandemic, the medical arena wrestled with major cybersecurity challenges, including insecure medical devices, protecting patient data and supporting outdated legacy equipment. COVID-19 has forced budget-strapped hospitals to address those systemic issues, and at the same time spurred new priorities around the digitization of healthcare services, telehealth rollouts and fending off an uptick in ransomware attacks.

Did I mention, this is all the while doctors and nurses are trying to save lives?

The healthcare sector isn't unique. Overnight, the COVID-19 crisis has changed the way companies in all sectors and regions do business. This eBook is relevant to any industry forced to reinvent themselves overnight – thanks to the coronavirus.

We examine emerging risks in the context of healthcare insecurity as a whole, and the growing risk for patients, doctors and the healthcare workers on the front lines. We examine medical-device security; the scourge of ransomware; the impact of a mass migration to telehealth; and the rise of medical espionage, as shadowy groups quest for competitive intel on COVID-19 vaccines and therapeutics.

Read on to find out what these risks mean for hospitals at the day-to-day level and how healthcare security teams can implement best practices to protect providers and patients. ■

Lindsey O'Donnell-Welch
eBook Guest Editor
Threatpost, Senior Editor
@LindseyOD123

Healthcare in Crisis: Diagnosing Cybersecurity Shortcomings in Unprecedented Times

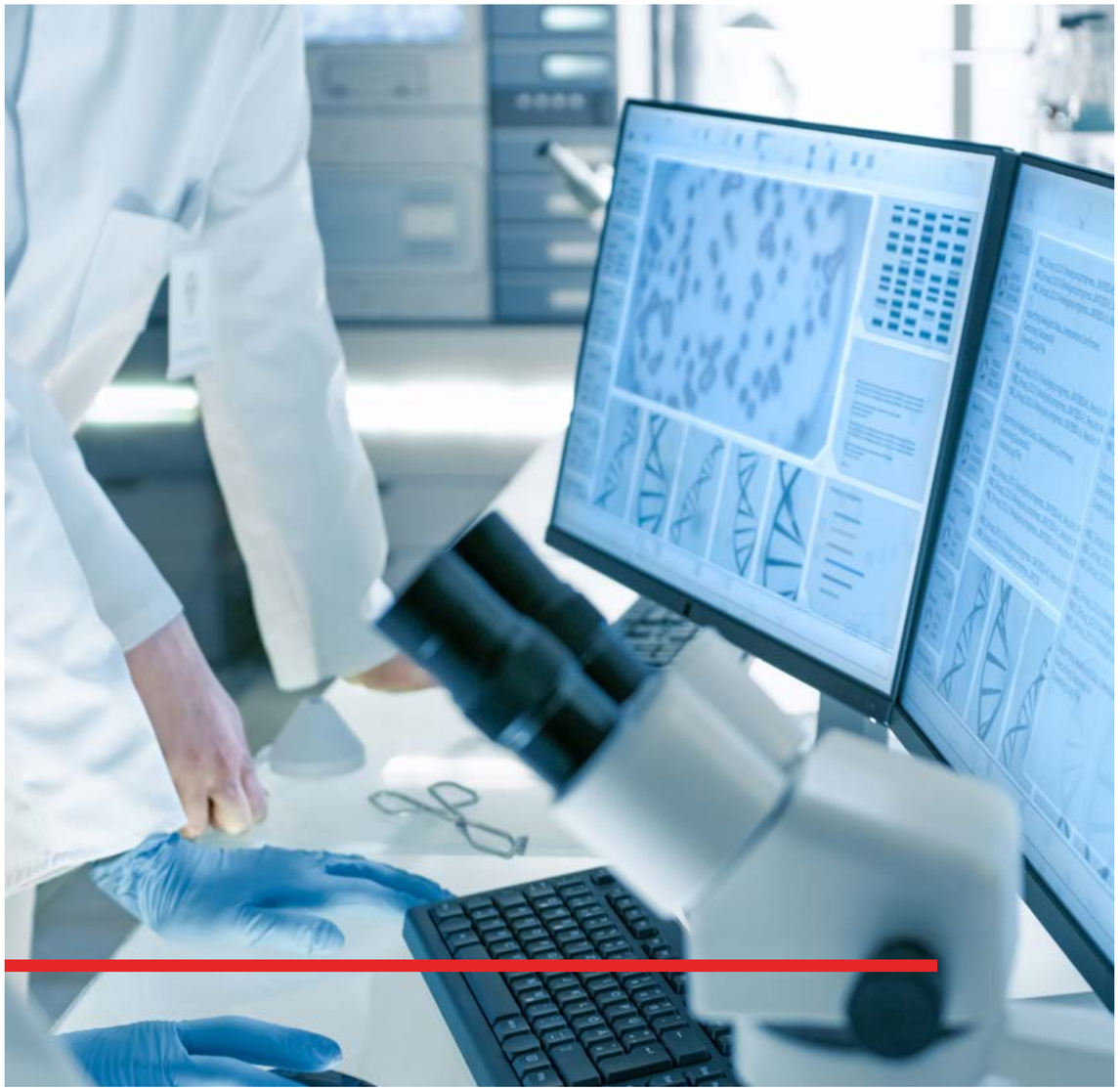
By Lindsey O'Donnell

When the COVID-19 pandemic first hit the U.S. hard in March, the Elmhurst Hospital was forced into a logistical nightmare.

It was a grim sign of the times, as the Queens, N.Y. hospital was flooded with hundreds of sick patients, with one medical resident describing conditions as "apocalyptic", according to a New York Times interview[1]. At the same time, hospitals also began a similar rush to increase capacity to keep up with growing infection rates, and scrambled to find personal protective equipment (PPE), ventilators and trained staff.

Lost in the chaos was IT security. In the early fog of the pandemic, cybersecurity took a back seat to keeping patients alive. But it did not take long before important hospital systems such as telehealth patient portals, backend billing and coding systems, connected medical devices and video-conferencing platforms were stressed.

Cybercriminals took notice. Cyberattacks targeting healthcare firms have increased 150 percent since the COVID-19 virus hit the U.S. shores[2]. The pandemic's unprecedented impact on healthcare lay bare the gaping holes in the healthcare industry's cybersecurity defenses. It is a sobering wakeup call that security experts say will have a lasting impact on the healthcare industry well into 2021.



Cyberattacks Target Vulnerable Systems

The goals for cybercriminals are varied. At one end of the spectrum, they're targeting personally identifiable information to be later used in credential-stuffing attacks or for resale on criminal black markets. At the other end, attackers have also launched costly ransomware attacks against insecure healthcare systems- potentially endangering patient lives.

"Frontline health professionals have been heroes during this pandemic, saving lives," said Beau Woods, a Cyber Safety Innovation Fellow with the Atlantic Council.

Woods, who has worked for the past 10 years with small hospitals, healthcare-focused nonprofits and government entities, added, "If technology goes offline, doctors and nurse practitioners can no longer give the quality of care that they were able to, or to as many people. Right now, with COVID-19, there's a dramatic rise in the attack surface and the number and types of systems that are being used," he said.

Healthcare Insecurity: A Chronic Condition

Of course, healthcare cyber-challenges aren't new. Security researchers have long pointed out myriad threats facing this critical industry segment.

For instance, the hospital equipment mix includes millions of insecure, single-purpose, connected medical devices, including insulin pumps and defibrillators, that are often open to hacks because they haven't been updated. Medical environments are also rife with critical infrastructure that runs on legacy platforms (such as Windows XP).

As an example of the magnitude of the outdated equipment problem, the Food and Drug Administration issued an emergency alert last year warning that Medtronic MiniMed insulin pumps are vulnerable to potentially life-threatening cyberattacks[3]. The flaw, which has since been patched, could have enabled cybercriminals to connect wirelessly to a MiniMed insulin pump and change its settings, allowing them to either deliver too much insulin, or not enough – with potentially fatal results for patients.

Another existing issue is the ongoing digitization of patient data and a growing reliance on connected medical devices. In general, this has created a massively expanded threat landscape for the healthcare industry[4].

Then there's the fact that there are millions of decentralized endpoints associated with telehealth – including patient facing portals, new COVID-related and existing mobile apps and wearables – all providing new ways to gather and process health-related data. As such, they crack open wide the attack vector for adversaries.

Financial Illness

With COVID-19, all of the existing issues that make healthcare cybersecurity difficult have become magnified, say experts.

For instance, telehealth adoption by primary caregivers jumped by 50 percent between January and June of 2020[5]. That required new investment in technology, when facilities are already paying a premium for testing, additional staff, PPE and ventilators.

"The biggest challenge with COVID-19 and healthcare security in my view is the significant strain on available resources," Jeff Tully, a pediatrician and anesthesiologist at the University of California at Davis, said. "With a precipitous decrease in elective surgical procedures and routine outpatient visits, hospitals and other healthcare factilities already facing razor-thin margins pre-pandemic are now forced to make increasingly difficult decisions about how to prioritize limited funds."

He points out that elective surgeries are a significant money-maker for hospitals, in normal times. Reuters news agency reported in March that the New York-Presbyterian Hospital postponed all elective surgeries, impacting 10 New York area hospitals.

These realities make it hard to advocate for something like a newly segmented network or increased IT security staffing, when healthcare workers may be furloughed or patient-care programs underfunded, he said.

Cyber-Infections Surge

While hospitals, doctors' offices and other healthcare stakeholders wrestle with a morass of cybersecurity challenges, threat actors have been paying attention – as evidenced by a cresting cybercriminal offensive on the healthcare industry.

A recent study by SecurityScorecard and DarkOwl found that attacks have increased 16 percent on web applications since the coronavirus pandemic hit states hard in March, while attacks on endpoints are up 56 percent and attacks targeting IP addresses have climbed 117 percent[6].

For hackers, COVID-19-related attack vectors remain low-hanging fruit. Patient data represents a lucrative store of goods to sell on the criminal underground. And ransomware attacks are all too easy, thanks to a lack of patching and user awareness/distraction – according to SonicWall, ransomware attack volumes have grown 109 percent annually in the U.S., in part due to the pandemic[7]. Espionage meanwhile continues as attackers strive to get their hands on valuable coronavirus treatment and vaccine research.

Real-world examples abound of cybercriminals taking advantage of the weaknesses. As an example, in 2019 a breach of AMCA impacted the data of 25 million patients – including their names, addresses, dates of birth and payment data[8].

Ransomware examples are readily available too. For instance, Hammersmith Medicines Research, a London-based healthcare provider that was working with the British government to test COVID-19 vaccines, was recently hit by a ransomware attack[9]. A ransomware attack in October also hit eResearchTechnology, a medical software company that supplies pharma companies with tools for conducting clinical trials – including trials for COVID-19 vaccines[10].

And on the espionage front, APT29, a Russia-based advanced persistent threat (APT) group also known as Cozy Bear, reportedly targeted academic and pharmaceutical research institutions in various countries around the world in July in just one of several such incidents[11].

Human Impact

With medical cybersecurity in a state of perpetual disruption – and ongoing attacks – there's a darker side to consider. Researchers and healthcare professionals alike worry that the heightened security threats are evolving from impacting technology availability and patient data privacy to actually threatening patients' physical safety.

The Atlantic Council's Woods cited academic research that examined the impact of re-routing ambulances around marathon race routes versus ambulances that did not face any obstructions[12]. That study determined that delays of just five minutes in care can impact patient outcomes.

A cyberattack's effect is no different, said Woods: A system-crippling incident can freeze access to care for hours, and sometimes days, he pointed out.

There's precedent for the concern. The WannaCry cyberattacks of 2017, which spread to more than 300,000 computers in 150 countries, not only brought down computer systems, but paralyzed hospitals' ability to keep customers' appointments, preventing patients' access to care[13].

"During WannaCry, in some areas many hospitals shut down, with at least 30 to 40 percent shutting down for a day to a week,"[14] said Woods. "If you think about someone with a stroke, with a 90-minute timeline of being treated, no one got the care needed during that time, which leads me to believe people have died because of these things before."

More recently, a ransomware attack on the Duesseldorf University Hospital in Germany led to the hospital turning away emergency patients. During this attack, a woman who had to be sent to a different healthcare facility, around 20 miles away, died. German prosecutors suspect it's because of delayed treatment after the cyberattack[15].

While the Duesseldorf University Hospital incident "might be the first smoking gun," Woods said, the incident is not the first death that's been caused – or at least partly influenced – by ransomware.

UC-Davis' Tully knows the potential human consequences of poor IT security in healthcare facilities first-hand. At a Black Hat USA session in 2018, Tully demonstrated a proof-of-concept attack against a computerized Health Level 7 lab-results system[16]. He was able to tamper with lab results coming from blood gas machines and urinalysis machines, which could lead to a lethal dosage of the wrong medication to treat an already sick patient.

"Certainly, sentinel events like WannaCry and, more recently, attacks explicitly directed at hospitals caring for COVID patients[17] raise the specter that the quality of care, particularly for time-critical conditions like heart attacks, strokes or sepsis, may be affected enough to result in increased morbidity and mortality," Tully said.

The Future of Healthcare Security

Against this bleak backdrop, the prognosis isn't all bad. There are several steps that healthcare organizations can take in order to secure patient data and critical infrastructure.

For one, in order to secure systems across the board, healthcare providers need to incorporate a patching cadence as an integral part of their vendor due diligence. In a report published in August, analyst firm McKinsey lists patching as the first in a list of required controls that healthcare organizations need to put into place[18].

Beyond that, hospital networks can bolster security by adopting proactive monitoring programs to weed out risks of breaches, conduct risk analyses to keep tabs on their connected devices and follow cybersecurity frameworks – like the National Institute of Technology (NIST) cybersecurity framework – to further understand new threats.

And, as is the case in many industries, prioritizing staff training and awareness across the organization is crucial — awareness can prevent spear-phishing and close other attack vectors. Building relationships between the IT teams and the hospital staff should also be at the top of the to-do list, Dan Costantino, CISO at Penn Medicine, said, stressing that hospital CISOs shouldn't "run programs in a vacuum."

He also urged IT teams to bring other business leaders to the table and give them "skin in the game." Doing so, he said, would help build strong security advocates within the business. This is particularly important during the ongoing pandemic, where security teams need the extra support of the healthcare leadership.

"The COVID-19 pandemic has been challenging for everyone, both personally and professionally," said Costantino. "Cybersecurity teams have found themselves in a position where business operations are changing at warp speed. COVID-19 presents the need to turn that known state of operations sideways as the business scrambles to adjust, and implement a model capable of responding to our communities' needs while maintaining employee safety." ■

By the Numbers: Telemed Risks and Best Practices

By Threatpost Staff

Healthcare organizations have gone virtual during the COVID-19 pandemic, just like the rest of us – with the use of telehealth services becoming the go-to format for med checks, routine consultations and therapist visits. But how safe are these services when it comes to patient data?

In an exclusive Threatpost poll of 159 participants (half of whom said they've had recent telemed appointments themselves), 72 percent saw an uptick in targeted cyberattacks on telehealth devices and networks over the past nine months. And more than half of those polled (58 percent) believe that virtual healthcare visits are risky, from a cybersecurity perspective.

Telehealth for many hospital IT departments represents new challenges. Many of them are already-overloaded and under-resourced in healthcare settings.

Our Threatpost poll found many are wrestling with the addition of technologies like Zoom (which has had its share of security issues and scrutiny) and secure delivery portals for HIPAA-protected data such as digital imaging and prescriptions. But also, telemed is a two-way street; patients at home are using home networks and personal devices to access their care – which can be much more susceptible to attackers than doctors' office infrastructure.

"Healthcare has had to make a lot of big, rapid moves around IT, including the forced transition to telehealth, and must rapidly respond to increased attention from malicious actors from nation-states right down to nuisance attackers," said Casey Ellis, CTO and founder of bug-bounty firm Bugcrowd.

In the past 9 months, have you seen an uptick in targeted cyberattacks on telehealth devices and networks?

Answer	Percent
No increase.	28,26%
5 to 25 percent increase	23,91%
25 to 50 percent increase	17,39%
50 to 75 percent increase	10,87%
75 to 100 percent increase	8,70%
Other	6.52%
1 to 5 percent increase	4,35%

Which are the most important cyber-health steps that organizations should prioritize?

Answer	Percent
Data integrity and proper cloud configurations	22,64%
Patching	21,31%
Third-party app vetting	20,75%
Endpoint protection	20,13%
Insider threats	13,21%
Other	1,26%

Of those poll participants who experienced an increase in attacks, 28 percent saw between a one- and 25-percent increase in cyberattack volume – with 37 percent reporting a snowballing of more than 25 percent.

When it comes to the risks that cybersecurity professionals are concerned about, more than half (58 percent) of respondents said that the biggest security challenges stem from the risk of data breaches as more patient information moves to the cloud (business email compromise and phishing attacks, insecure APIs and ransomware were other challenges mentioned).

But virtual healthcare and telehealth services are also top of mind when it comes to risks, with half of the respondents indicating they have had a telemed appointment since the pandemic broke out.

When asked what they view as the riskiest link in the virtual healthcare chain, 35 percent of Threatpost poll respondents pointed to insecure video-conferencing platforms. This was followed by the telemedicine platforms used to manage devices and patient data (25 percent); the digitization of patient data (17 percent) and purpose-built telemed IoT devices (11 percent).

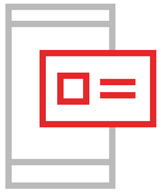
Threatpost also asked about the biggest cybersecurity challenges when it comes to telehealth – and an overwhelming majority (58 percent) cited preventing data breaches as more patient information moves to the cloud. A quarter (24 percent) of respondents said that thwarting business email compromise and phishing attacks is the biggest challenge, while wrestling with insecure APIs and ransomware were also cited by some.

On the positive side of the equation, respondents cited their favorite best practices for security teams in healthcare organizations to take on.

What are the riskiest links in the virtual healthcare chain?

Insecure video-conferencing platforms **35%**

The telemedicine platforms used to manage devices and patient data **25%**



The digitization of patient data **17%**

Purpose-built telemed IoT devices **11%**

Almost a quarter (23 percent) pointed to data integrity and proper cloud configuration – which dovetails with the prevailing feeling that cloud security is the biggest telemed challenge. Another 21 percent mentioned patching, long considered a bedrock requirement for security in any environment; and yet another 21 percent pointed to third-party app vetting. Lastly, 20 percent mentioned endpoint protection, while 13.2 percent said protecting against insider threats should be a priority.

And finally, those polled were asked which healthcare segments is the best prepared when it comes to telemed cybersecurity. More than a third (36 percent) put their faith in medical insurance, medical services and managed care; while pharmaceutical and related segments got the seal of approval from 27 percent of respondents. Healthcare services and facilities didn't fare as well, with a mere 16 percent citing hospitals and the like as secure for telemed; and medical devices, equipment and hospital-supply manufacturers fared even worse, cited by just 13 percent of respondents. ■

Ransomware Attacks on Hospitals: When Malware Gets Deadly

By Tara Seals

Despite hospitals being on the front lines during the pandemic, bad actors have continued to target them with ransomware. In addition to wreaking havoc on operational processes in medical facilities at the worst possible time, the attacks have evolved to threaten patient safety.

In September, employees at Universal Health Services (UHS), a Fortune-500 owner of a nationwide network of hospitals, reported widespread outages that resulted in delayed lab results, a fallback to pen and paper, and patients being diverted to other hospitals. The culprit turned out to be the Ryuk ransomware, which locked up hospital systems for days[19].

"No patients died tonight in our [emergency room] but I can surely see how this could happen in large centers due to delay in patient care," a Reddit user identifying themselves as a nurse, wrote at the time.

The concern isn't overblown. Earlier that month, a ransomware attack at a Dusseldorf University hospital in Germany resulted in emergency-room diversions to other hospitals. According to a report by the Ministry of Justice of the State North Rhine-Westphalia, a patient died who had to be taken to a more distant hospital in Wuppertal because of the attack on the clinic's servers[20].

This turn of events comes after several ransomware gangs actually pledged not to hit hospitals because of the ongoing COVID-19 scourge. The Maze and DoppelPaymer groups, for instance, said they would not target medical facilities and, if accidentally hit, would provide the decryption keys at no charge. The Netwalker operators, meanwhile, said they would not target hospitals, however if accidentally hit, the hospital would still have to pay the ransom.

Other groups have less scruples, and in fact, some (like Netwalker) have reneged on their pledges. In fact, incidents of ransomware attacks against hospitals skyrocketed in October. So much so that, the U.S. Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the U.S. Department of Health and Human Services issued a security bulletin warning of "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[21] Among those hit lately include well-known facilities like University Hospital in New Jersey, Boston's Children's Hospital and Children's Hospital in Little Rock.

"The promise not to attack hospitals was always an empty one given the number of players in the ransomware game that would not restrain from it," said Erich Kron, security awareness advocate at KnowBe4. "Spanish hospitals were targeted by Netwalker campaigns using COVID-19 related messaging in the attacks, although promising not to."

The poor outcomes around patient diversions are a sign of the cyber-times, according to Heather Paunet, senior vice president at Untangle.

"We all trust that hospitals have the ability to address any life-threatening case or create a sense of stability before transferring patients for additional care,"

she said. “It does bring to light the synergy between medical professionals and technology used to create that patient stability.”

And to that point, patient diversions may not be the most worrying aspect of ransomware’s impact on physical well-being.

“Any time malware infects a hospital to the point that systems have to be taken offline, or that records are unavailable, this poses a risk to the patients’ safety,” Kron said. “From potential drug interactions to allergies, the information is vital to doctors, nurses and support staff, such as anesthesiologists, to ensure the safety of patients. The loss of access to patient data is the biggest threat to patients’ safety.”

It’s clear that cybersecurity best practices should also be medical best practices. But the ransomware epidemic has exposed plenty of unhealthy habits among hospitals nationwide. For instance, the American Hospital Association has reported a big uptick in phishing emails laden with malware and malicious links, often themed with promises of N95 masks for sale or even the availability of lifesaving ventilators[22]. This is the initial attack vector for many ransomware attacks, likely including the UHS incident[23].

Also, many facilities don’t have backups, as was seen in a recent attack on a vaccine research facility[24].

“With each ransomware attack on a hospital or medical center, it becomes increasingly clear that back-up plans are being developed or initiated as an immediate response while networks are down,” Paunet said.

Fortunately, there are prescriptions for avoiding the worst that ransomware has to offer, starting with putting the aforementioned plans in place immediately – including remote or offline patient data backups.

Also, since ransomware is typically spread through email phishing or through attacks on remote-access methods, Kron noted that organizations can greatly benefit from focusing on email phishing defenses.

"This includes a serious assessment of current controls in place and the state of their employee awareness training, and securing and monitoring remote-access options," he said.

Paunet also noted that medical instruments, such as ventilators, insulin pumps and other internet-of-things (IoT) devices that may be unpatched or outdated can become vulnerable network-access points.

"These devices need to be audited constantly for software updates, patches and other upgrades to ensure that outdated software isn't leaving the network open for criminals," she said.

And finally, like any organization, hospitals must look to build barriers against ransomware while understanding that cybercriminals continue to improve their tactics. The spate of attacks in the medical arena is unlikely to wane soon, so organizations should assume they're being targeted – especially since paying the ransom is not uncommon[25].

"As healthcare pays ransoms and the large dollar amounts they pay are highlighted in the news, this becomes an indication that this is a sector that is willing to pay. Attackers set their targets and evolve their techniques where they feel they will be most successful," Paunet said. ■

Hackers Look to COVID-19 IP Theft

By Tara Seals

Attackers are looking to the healthcare space as a rich repository of intellectual property (IP) now more than ever, as critical research of COVID-19 therapeutics and vaccine candidates continues. Several incidents show that nation-states are targeting biotech companies with a vengeance, as the quest to beat the pandemic continues.

COVID-19 manufacturer Dr. Reddy's Laboratories suffered an attack in October which forced it to shut down plants across Brazil, India, the U.K and the U.S. The Indian-based company is contracted to manufacture Russia's "Sputnik V" COVID-19 vaccine.

In July, the U.S. Department of Homeland Security (DHS) warned that Russia-linked group APT29 (a.k.a. Cozy Bear or The Dukes) has been targeting British, Canadian and U.S. research companies[26]. The advanced persistent threat (APT) group looks to pilfer COVID-19 vaccine research from academic and pharmaceutical institutions, in a likely attempt to get ahead on a cure for coronavirus, DHS warned.

Earlier in the pandemic, the World Health Organization was targeted by the DarkHotel APT group, which looked to infiltrate its networks to steal information[27].

Similarly, the U.S. Justice Department recently accused Chinese-sponsored

cybercriminals of spying on COVID-19 researcher Moderna, which just announced a vaccine that appears to be almost 95 percent effective.

“Even if you are good at science, this is a cheap insurance policy to maintain a seat at the table for the game of nations,” said Sam Curry, Cybereason CSO. “The headlines around stealing vaccine research, data and information being used to create vaccines to the world’s pandemic should be a wakeup call to research firms and both the private and public sector. It is not a question of if hacking will be done, but rather how much has already taken place.”

He added that nation-state backed crime groups are well funded, patient and highly skilled at their craft – meaning there’s likely more activity going on than meets the eye. After all, having a lead on “re-opening” their part of the world could come with a lasting balance-of-power impact.

“Some groups have likely infiltrated these companies and have not been caught, and are pilfering through specific vaccine information, patents and other valuable content,” he said. “A vaccine for COVID is a strategically valuable (maybe crucial) asset. Whoever gets a vaccine first has an economic advantage and it is worth billions of dollars to a country and its economy. It is the ultimate IP with immediate value.”

In terms of how APTs are infiltrating their targets, commercially available trojans like Emotet or Trickbot are designed for enterprises and complex environments, according to Rob Bathurst, CTO of cybersecurity firm Digitalware. These backdoors can gain persistence and provide a deployment platform for making further inroads into a victim’s network.

“The rule of thumb for an attacker is to use just enough to get the job done–

and that is usually commercial malware first, and custom packages only if needed for a specific target," he said.

Custom kits have indeed been spotted. DHS for instance warned that APT29 is using advanced, custom malware called "WellMess" and "WellMail" for data exfiltration.

As far as safeguarding the IP jewels, best practices start – as ever – with the basics. One of the most common ways for criminals to gain access to any computer network is through phishing – clicking on a dodgy email is all it takes for a threat actor to drop one of the aforementioned backdoors. It's a tactic that was seen this year being deployed in the WHO attacks; a phishing page mimicked the WHO's internal email system and looked to steal passwords from multiple agency staffers.

"To combat this type of attack, organizations need to continue to improve their security hygiene, implement around-the-clock threat hunting and increase their ability to detect malicious activity early," Curry said. "Security-awareness training is also needed and employees should not open attachments from unknown sources and never download content from dubious sources."

When it comes to preventing malware, "no security solution is perfect," Bathurst said. "The only way to have a chance to prevent IP theft is to prevent the initial compromise and minimize the damage from the point of impact."

To that end, organizations can use modern antivirus protections with a combination of behavioral analytics/pattern matching, binary analysis and pre-execution analysis. And, organizations should regularly review the configurations and capabilities of network-based defense technologies, beyond just firewall rules.

It's also critical to consider the supply chain, Bathurst added. This includes researchers, government agencies, universities, pharma, hospitals treating cases, and companies involved in the manufacturing of ingredients.

For instance, in November, global biotech firm Miltenyi said that it had been battling a malware attack. It's supplying SARS-CoV-2 antigens for researchers working on treatments for COVID-19.

"If the attacker is after vaccine-related data, that could come from third-party researchers with access to your data, your clinical trials database, your research team, their home computers, notes on tables, laboratory equipment memory or storage, and even the industrial control systems that control the drug-manufacturing plants," Bathurst explained. "Ultimately, it comes down to understanding your risks and impact points."

Above all, it's clear that the stakes are too high for the espionage onslaught to dry up anytime soon – and in fact, the worst could be yet to come, researchers suggest.

"As flu season descends upon us and vaccine research continues to progress through Phase 3 trials, I would expect to see a sharp increase in actor activity beyond what has already been reported," Bathurst said. "It's in the interest of nation-state intelligence agencies to continue to leverage everything they can throughout their ecosystem to harvest information." ■

Medical Device Security: Diagnosis Critical

By Tom Spring

A hacked insulin pump is the last thing a diabetic wants to worry about when life-saving fluids are pumped into their body. Sadly, concerns about medical-device IT security are a healthcare reality.

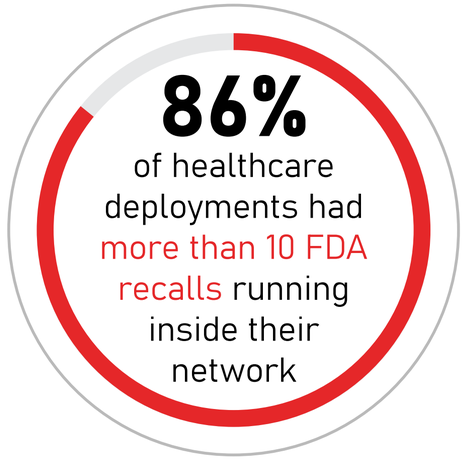
So far in 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued more than a half-dozen warnings tied to connected drug pumps alone. Vulnerabilities found in pumps made by Baxter International[28] and Becton Dickinson Alaris System, for example, could be exploited to launch a DDoS attack, alter system configurations or siphon off patient data.

The Diagnosis

Cybersecurity has also become a major theme for the Federal Drug Administration, which oversees medical-device safety. Since January, the FDA has issued a flurry of warnings urging medical device-makers and hospitals to patch their hardware against a slew of vulnerabilities, ranging from SweynTooth and URGENT/11[29] to Ripple20 and SigRed.

Ripple20 for instance is a group of bugs found in June[30], plaguing 53,000 medical device models. The flaws give remote attackers the ability to execute remote code, according to Forescout research.

A year-long analysis of 5 million internet-of-medical-things (IoMT) devices found that 86 percent of healthcare deployments had more than 10 FDA recalls running inside their network, according to Ordr[31]. Recalled IoMT devices can be considered either defective, posing a health risk or both.



Underlying Symptoms

Experts warn medical-device security is a chronic problem, now exacerbated by COVID-era healthcare challenges. Hospitals have been forced to prioritize budgets and staffing to focus on lifesaving care - meaning that IT security often takes a back seat. Adding insult to injury, hackers are aware of this, and are also now capitalizing on these healthcare strains with a barrage of ransomware attacks, phishing attacks and more.

Universal Health Services was one of several hospital networks hit this year with ransomware attacks[32], causing major day-to-day disruptions to over 400 facilities across the U.S., Puerto Rico and United Kingdom. According to Tom August, a longtime CISO in the healthcare field, the medical-device aspect of such disruptions can't be ignored.

"The likelihood is low, but there is a really high potential impact if one of these devices is attacked," August said. "Maybe you put ransomware on my

computer. That's bad. But if you have malware on a medical device that a patient hooked up to, there is tremendous, wide-open risk to human life."

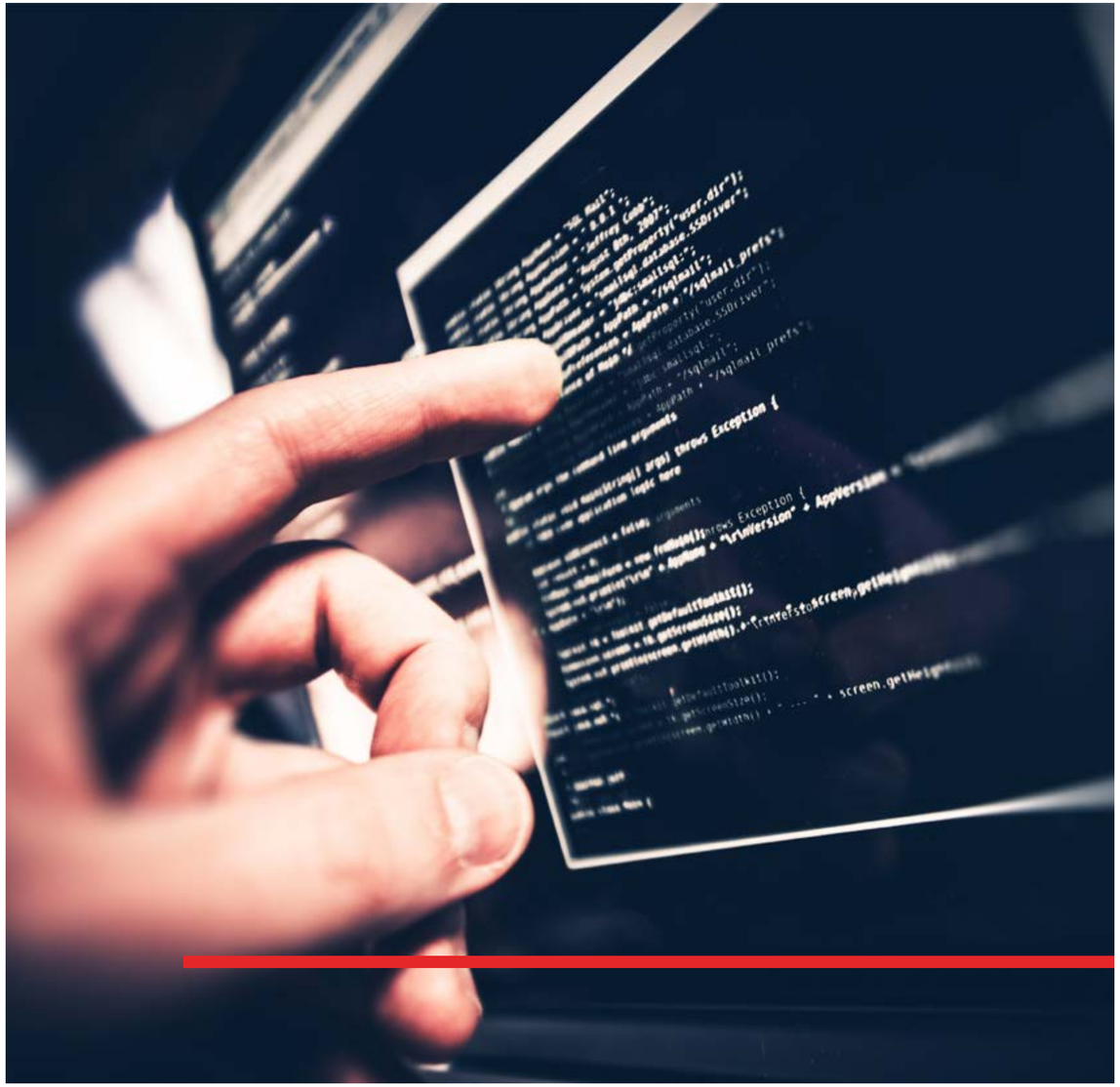
Medical History

It should be recognized that medical-device security has long been a challenge, suffering the same uphill management battle that the entire sprawling mess of IoT gadgets has faced. That is, a lack of security-by-design, unclear mechanisms for patching and updates, and the potential for configuration mistakes (like forgetting to change default passwords).

"The coronavirus isn't creating more vulnerabilities in medical devices, it's laid bare the problems that already exist," said Tim Erlin, vice president of product management and strategy at Tripwire.

The segment also faces some unique challenges. For instance, because of strict FDA guidelines over device configuration and legally-binding vendor support contracts, patient-care facilities often must rely on slow-to-move vendors for patching, upgrades and replacements - a rare and expensive process.

"Medical devices are a blind spot for hospitals," August said. "In many cases, hospitals can't manage the devices – vendors do. We can't patch them, because vendors won't allow it. We can't install anti-malware protection because vendors say it breaks the warranty."



The Cure

Reducing medical-device cybersecurity risks may be especially challenging, but there are some best practices that can help.

Taking a medical-device inventory is a first step at identifying the scope of the cybersecurity challenge. The Ordr study found that 51 percent of IT teams are unaware of what types of devices are touching their network.

Ordr also discovered Facebook and YouTube applications running on MRI and CT machines — which were also running legacy and unsupported operating systems like Windows XP.

"Using medical devices to surf the web puts the organization at a higher risk of falling victim to a used ransomware and other malware attacks," according to the report.

Meanwhile, suggestions for locking down IoMT devices include assessing a device's exposure to the internet, disabling unnecessary or unused services on devices and segmenting critical networks by IoT-device needs. ■

For this large healthcare technology solutions company, product security is paramount given the nature, use and criticality of its products, and stringent compliance requirements. The Application Security Officer and his team are using the ZeroNorth application security automation and orchestration platform to gain a strategic, holistic view of AppSec and compliance—comparing vulnerability findings across applications and scanning tools, surfacing persistent AppSec problems and assessing risk for critical business assets. Read the full Case Study here.

Conclusion

The healthcare industry is consistently targeted by cybercriminals, because it has unique security challenges that widen the attack surface – and unique assets that can be turned into cash or geopolitical advantage.

Beyond the threat to patient data and intellectual property, ransomware attacks against hospitals are cresting, which is particularly concerning against the backdrop of the COVID-19 pandemic.

Security defenders are actively working on implementing best practices and technology solutions to protect hospitals, clinics, labs and more. But ongoing innovation on the part of attackers turns the state of play into an arms race, and it's one that isn't going away anytime soon.

It's essential for healthcare security teams to lock down connected medical devices, manage patient digitization and telehealth rollouts with security in mind, and put IT resources into basic fundamentals like network segmentation and patching. And in the context of the coronavirus, there is an even more urgent need for better countermeasures to prevent attacks that threaten patients, doctors and healthcare workers on the front lines.

Understanding what the risks mean for hospitals at the day-to-day level, and how healthcare security teams can implement best practices to protect doctors and patients, will serve organizations well in the COVID-19 era, and well into the future. ■

Acknowledgments

Editorial

Tom Spring
Editor in Chief
thomas.spring@threatpost.com

Tara Seals
Senior Editor
tara.seals@threatpost.com

Lindsey O'Donnell-Welch
Senior Editor
Lindsey.odonnell@threatpost.com

Sponsorship Inquiries

Clare Liberis
Business Development Manager
clare.liberis@threatpost.com
+1-781-888-2248

Threatpost
www.threatpost.com

Copyright 2020 Threatpost

References

1 https://www.nytimes.com/2020/03/25/nyregion/nyc-coronavirus-hospitals.html

2 https://www.medicaldevice-network.com/news/coronavirus-cybersecurity/

3 https://threatpost.com/medtronic-defibrillators-have-critical-flaws-warns-dhs/143068/

4 https://www.mobihealthnews.com/content/report-global-telemedicine-market-will-hit-130b-2025

5 https://www.hhs.gov/about/news/2020/07/28/hhs-issues-new-report-highlighting-dramatic-trends-in-medicare-beneficiary-telehealth-utilization-amid-covid-19.html

6 https://s3.amazonaws.com/ssc-corporate-website-production/documents/resources/healthcare-industry-telehealth-cybersecurity-report.pdf

7 https://threatpost.com/sharp-spike-ransomware-pandemic-inspires-attackers/157689/

8 https://threatpost.com/amca-healthcare-hack-widens-opko/145453/

9 https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

10 https://threatpost.com/covid-19-clinical-trials-ransomware/159877/

11 https://threatpost.com/state-sponsored-hackers-steal-covid-19-vaccine-research/157514/

12 https://www.nejm.org/doi/full/10.1056/NEJMsa1614073

13 https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/

14 https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suffered-from-attack-past-6-months

15 https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

16 https://threatpost.com/black-hat-2018-with-healthcare-security-flaws-safetys-increasingly-at-stake/134905/

17 https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

18 https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/How%20six%20companies%20are%20using%20technology%20and%20data%20to%20transform%20themselves/The-next-normal-the-recovery-will-be-digital.pdf

19 https://threatpost.com/universal-health-ransomware-hospitals-nationwide/159604/

20 https://abcnews.go.com/International/wireStory/german-hospital-hacked-patient-city-dies-73069416

nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

21 https://threatpost.com/hospitals-hit-by-ransomware/160695/

22 https://www.aha.org/center/emerging-issues/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

23 https://www.pcmag.com/news/ransomware-hits-healthcare-provider-uhs-shuts-down-hospital-it-systems

24 https://threatpost.com/covid-19-clinical-trials-ransomware/159877/

25 https://digitalguardian.com/blog/following-ransomware-attack-indiana-hospital-pays-55k-unlock-data

26 https://threatpost.com/state-sponsored-hackers-steal-covid-19-vaccine-research/157514/

27 https://threatpost.com/who-attacked-possible-apt-covid-19-cyberattacks-double/154083/

https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl/exclusive-chinese-backed-hackers-targeted-covid-19-vaccine-firm-moderna-idUSKCN24V38M

28 https://us-cert.cisa.gov/ics/advisories/icsma-20-170-04

29 https://threatpost.com/urgent-11-critical-infrastructure-eternalblue/146731/

30 https://threatpost.com/millions-connected-devices-ripple20-bugs/156599/

31 https://ordr.net/wp-content/uploads/Rise-of-the-Machines-2020-Enterprise-of-Things-Adoption-and-Risk-Report.pdf

32 https://threatpost.com/universal-health-ransomware-hospitals-nationwide/159604/

threatpost | Insider eBook

November 2020