HealthManagement.org

LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 6 • € 22

ISSN = 1377-7629

Cybersecurity: Preventing the Worst-Case Scenario

THE JOURNAL 2022

Challenges, Strategies and Recommendations to Improve Cybersecurity

Dan Brown | Chief Technology Officer | Agfa HealthCare
Tim Hill | Global Security and Privacy Program Manager | Agfa HealthCare
Jarius Jackson | Data Protection Officer & Security & Privacy Tech Specialist | Agfa HealthCare

Cybersecurity is vital for the effective functioning of healthcare organisations and protecting private and important patient information and data. HealthManagement.org spoke to Dan Brown, Chief Technology Officer, Tim Hill, Global Security and Privacy Program Manager and Jarius Jackson, Data Protection Officer & Security & Privacy Tech Specialist at Agfa HealthCare, to discuss the main challenges customers face regarding cybersecurity and what strategies they can implement to protect themselves against cybersecurity attacks.

Key Points

- A major ransomware attack can cripple an organisation and cost millions of dollars/Euros to recover from.
- Each healthcare organisation should create principles to be secure by default and by design.
- A single, unified enterprise-wide image management system not only provides health systems with improvements in productivity and workflows, but also reduces the total number of systems handling sensitive data.
- Agfa HealthCare's security patch management policy keeps the confidentiality, integrity and/or availability risks introduced by security vulnerabilities under control to help protect patient safety and privacy.
- Agfa HealthCare became one of the first companies to be named Cybersecurity Transparent Leader by KLAS Research and Censinet, recognising the company's willingness to continually improve cybersecurity maturity and support customers in the delivery of safe and secure patient care.

What are the main challenges and worries of your customers with regard to cybersecurity? Are the issues customers are facing similar around the globe? Or do you see differences?

Dan Brown: Major ransomware attacks are a key concern of our customers. A major ransomware attack can cripple a health organisation and cost millions of dollars/Euros to recover from – if at all, depending on their preparedness for major events. We have found through customer meetings that some customers are quite well prepared for business continuity scenarios, like a fire in a data centre, but not always equally prepared for ransomware attacks. Agfa HealthCare is continuing to find new ways to work with our customers to create both the awareness and the playbook that is periodically practiced for what to do in event of a cyber emergency.

Do customers take cybersecurity risks seriously enough? Is it a top priority for your customers?

Tim Hill: It's on the minds of most organisations, regardless of their size. The challenge most organisations have is that they are often confronted with difficult trade-offs on how they spend their limited resources.

The reality is that malicious actors are out there, and they are getting more and more crafty. This constantly challenges organisations like Agfa HealthCare, our partners, and our customers. They have to be pragmatic and determined in their defence, approach, business planning and strategic

alliances with partners, vendors, and suppliers, to make sure that if an unfortunate event happens, they can recover from it quickly to enable their systems and the services they provide to continue to be available. This is something Agfa HealthCare itself truly targets, making sure we're supporting the delivery of the best patient care and a stable and secure solution so that our customers will look at us with confidence and trust.

From a holistic and preventive point of view, how does Agfa team up with its customers to provide a secure solution?

DB: With a single, unified enterprise-wide image management system, health systems not only have improvements in productivity and workflows, but they also reduce the total number of systems handling sensitive data. This means they have fewer gates to guard, with fewer access points and fewer opportunities for breach. Without Agfa's Enterprise Imaging, most customers have several different departmental solutions and even individuals storing data on their local PCs – each of which has to be secured by the hospital's IT staff. The unified Enterprise Imaging Platform also reduces the time that most hospital IT teams spend. Money is not wasted integrating multiple solutions and manually transferring data from siloed locations, simplifying the normally complex world of imaging information management. This allows Agfa's customers to focus security efforts and resources where they will have the most impact.

More practically, how are you helping your customers, which include large hospital networks, to protect themselves against cybersecurity attacks?

Jarius Jackson: We created a ransomware playbook that is both internally and externally facing. We have been meeting with customers to understand their concerns and challenges and offer advice. We developed and posted the Security Vulnerability Notifications for Enterprise Imaging on Agfa's customer portal for transparency and communication. We developed an SBOM (Software Bill of Materials) showing all of the components used in our software well ahead of when it will become mandatory in the U.S. We created additional tooling and process improvements to provide better visibility into not only Agfa's homegrown-software but also the potential vulnerability impact of third-party libraries and components used with the EI system.

As part of Agfa's vulnerability management programme, Enterprise Imaging systems are hardened using Security Technical Implementation Guidelines (STIG) from the Centre for Internet Security (CIS) and the Defense Information Systems Agency (DISA). Before delivery to customers, each system is scanned at both the operating system and application level, using industry standard tools. Through means of static code analysis, refresh training for development staff, and a targeted focus on OWASP development principles, Agfa HealthCare has increased its vigilance being secure by design.

With a single, unified enterprise-wide image management system, health systems not only have improvements in productivity and workflows, but they also reduce the total number of systems handling sensitive data

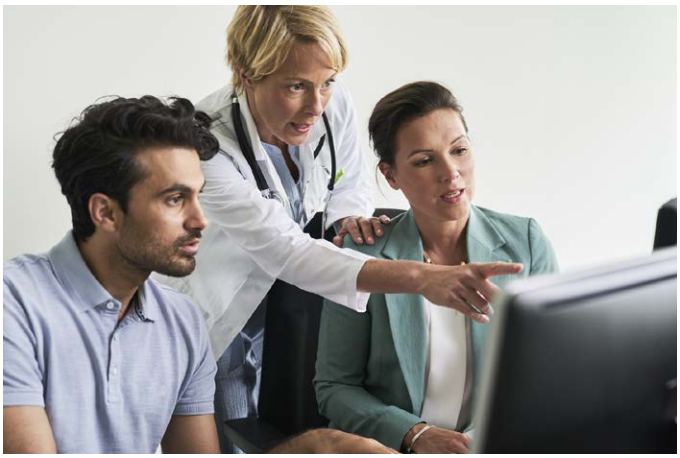
How do you keep up to date with ever-evolving security threats? How do you manage to stay ahead of the threats?

TH: Constant vigilance. This takes consistent and sustained effort from our teams inside Agfa HealthCare to stay on top of the constantly evolving landscape of security threats. We regularly scan our product for new vulnerabilities in our code and in all third-party add-ons we sell. We create our solutions to be safe by design, and we keep rigorous training for our employees, so they are at the top of their game to secure our customers.

You collaborate with KLAS Censinet on their Cybersecurity Transparency Leader initiative. Can you explain a bit more about this initiative?

JJ: KLAS Research and Censinet are strategic partners on a joint mission to improve cybersecurity preparedness in healthcare. They aim to help healthcare IT vendors and services firms improve their overall risk and security profile by driving greater trust and transparency to thousands of

healthcare providers. They have assessed and rated more than 130 healthcare products on the Censinet RiskOps platform. Agfa HealthCare became one of the first companies to be named Cybersecurity Transparent Leader by KLAS Research and Censinet. This award recognises our company's willingness to share and continually improve overall cybersecurity maturity and our commitment to supporting customers in delivering safe and secure patient care. This isn't a one-time certification, but something we must stay on top of and work to improve upon each year.



There are several ISO certifications that include cybersecurity topics and a series of regional privacy regulations that you must consider. Does this multitude of regulations complicate your work with regard to cybersecurity and prevention?

TH: While Agfa HealthCare is committed to investing in what is needed to stay on top of all of these certifications, we also look to work smart, not just hard. Despite the variety of certifications, most are core security principles, so we commit to certifications where required in the regions we do business in. We prioritise the privacy and handling of sensitive data and ensure our solutions are designed and implemented to enable healthcare organisations to provide the best and most secure patient care possible.

As a conclusion, what would be your recommendations for hospitals and healthcare professionals to protect themselves from cybersecurity attacks?

TH: Each healthcare organisation should create principles to be secure by default and by design. Work with your IT partners to design a robust and secure solution upfront. As mentioned at the beginning, our experience from customer meetings, both before and after ransomware attacks, is that they usually cater quite well for disaster scenarios, like a fire in their data centre, but less so for ransomware attacks. Some practical advice and best practices include:

- Wherever possible, reduce complexity by minimising the number of unique systems.
- Make sure that your backups are segmented from your production infrastructure. We recommend investigating in immutable backup options.
- Regular vulnerability tests for systems exposed to the outside (i.e. penetration tests).
- Effective system life cycle management - keep your systems current in terms of supported versions. Too often, we see cases where legacy systems are still being used, running on unsupported platforms with no security updates.
- Awareness training for staff – In most organisations, mistakes made by individuals via phishing or loading unauthorised software or media from outside their organisation are the most commonly exploited entry points, not always high-tech hackers like we see in the movies.
- Develop Business Continuity Plans (BCP) to include a cyber-attack scenario.
- Invest in cyber insurance.
- Also, we recommend that organisations should dedicate 10-15% of their IT budget to Information Security and Privacy initiatives.
- Consider gaining a security certification like ISO 27001. The focus of the ISO 27001 standard is on a company's Information Security Management System (ISMS), which outlines how they have integrated information security into its business processes. ■

HealthManagement.org

Promoting Management and Leadership