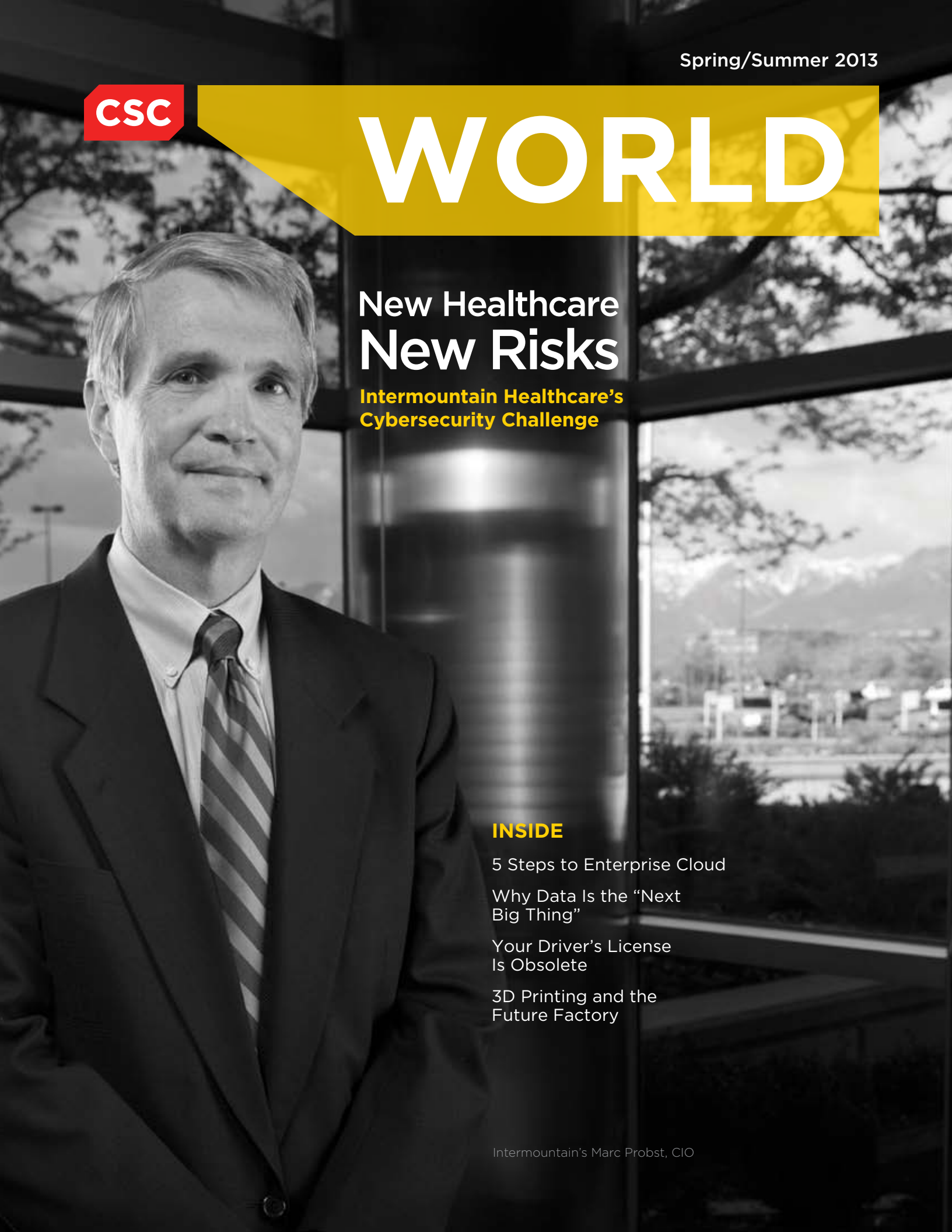
Spring/Summer 2013

CSC

WORLD

New Healthcare New Risks

Intermountain Healthcare's Cybersecurity Challenge



INSIDE

Intermountain's Marc Probst, CIO

New Healthcare. New Risks.

Intermountain Healthcare's Cybersecurity Challenge

by Jenny Mangelsdorf

The healthcare industry is venturing into a world of tremendous opportunity — and tremendous risk. By linking systems and medical devices to the Internet, adopting electronic health records and implementing regulatory reforms, the industry is drastically improving healthcare for all of us. But the changes are also creating a health IT landscape fraught with security challenges.

While attacks on the healthcare industry aren't as high-profile as those experienced by the financial services and energy sectors, security experts say cybercriminals have increased their assaults on critical medical systems to steal valuable patient data.

Surveys show that most health organizations have suffered some kind of data breach or security incident. For example, Ponemon Institute's Third Annual Study on Patient Privacy reveals 94% of the healthcare organizations it interviewed reported at least one data breach in the past two years, and 45% said they had more than five breaches during that time.

With risks continuing to escalate, some organizations are taking a proactive approach, working to better protect patients' data and fortify their systems before an attack or theft occurs.

One organization keen on building greater resiliency and security is Intermountain Healthcare, a health system repeatedly honored for excellence and innovation both in healthcare and its use of technology. Last year, CSC began working with Intermountain to help strengthen its security. Along the way, the team has applied innovative approaches to better secure Intermountain's network of systems and data.

Managing risk with innovation

Intermountain Healthcare is a nonprofit health system based in Salt Lake City, Utah, consisting of 22 hospitals, 185 physician clinics, an affiliated health insurance company and 33,000 employees that serve the state of Utah and southeastern Idaho.

"Intermountain Healthcare has a long legacy of very high quality in healthcare and, from a cost perspective, we are one of the lowest-cost providers of healthcare in the country," says Marc Probst, chief information officer and vice president of Information Systems at Intermountain Healthcare. "That comes from a focus on using systems and really smart people taking the data from these systems and making good decisions. In areas like privacy and security, though, we are looking to other industries."

Client: Intermountain Healthcare

Challenge

- Growing use of vulnerable, complex medical technologies, mobile devices and medical diagnostic devices with IP addresses
- Escalating healthcare focus by cybercriminals, partially due to increased black-market value of patient medical records
- Evolving regulations carrying both legal and financial penalties

Solution

- Data classification, identification, encryption and enclaving
- Audit preparedness
- Revised security policies, procedures, guidelines and training

Results

- An innovative scalable, self-healing, controlled and managed network infrastructure design that protects data, applications and systems
- Greater resiliency and security to protect patients and thwart current and emerging cyberthreats
- Creative information security awareness, training content and delivery

Read more CSC client success stories at csc.com/success_stories.

Information systems security and privacy ranks a close second in the top challenges facing healthcare CIOs after attaining effective meaningful use of electronic medical records, adds Probst. "Regulation changes and the complex nature of medical services create a huge security and privacy challenge."

Cybercriminals' increased focus on healthcare data compounds that challenge. Intermountain wanted to ensure that it was reducing the risk to its organization and that it stays current with the latest security controls.

"The dynamic has changed substantially," says Ashif Jiwani, CSC Global Cybersecurity partner, Healthcare. "A year ago, the financial services industry was attacked from everywhere in the world; now the healthcare industry has become the easiest target for commercial hackers."

For cybercriminals, stealing identities from sick people is fairly easy since they're focused on getting well and many times let other responsibilities slip, such as ensuring that their identities haven't been stolen. Healthcare records, which contain megabytes of valuable personal data ranging from Social Security numbers to blood types, have also become more valuable than simple credit card numbers, which financial industries have worked hard to protect with antifraud capabilities.

"Through CSC's global threat intelligence, we are constantly watching the black-market exchange boards to see what's happening on behalf of our clients," says Tom Patterson, CSC Global Cybersecurity Consulting general manager. "Currently, criminals are getting an average of $2 for a credit card record, whereas a medical record brings about $20."

An issue of reputation and regulation

At $20 a record, criminals can quickly make a lot of money and simultaneously damage an organization's reputation and budget. Take last year's attack on the state of Utah's Department of Technology Services computer server, which stores Medicaid and Children's Health Insurance Program claims data. Cybercriminals stole 280,000 Social Security numbers and "less sensitive" personal information of another 500,000 people. The Utah department is still dealing with the fallout.

Marc Probst, CIO and VP of Information Systems, Intermountain

Karl West, CISO, Intermountain

"Until a breach occurs, security usually tends to be an afterthought," says Jiwani. "Intermountain has decided that's not where it wants to be. The system has made security a priority because it feels that the protection of its patients' information and privacy as well as its reputation is as important as any of its other prime strategies."

State and federal regulators also have strong feelings about securing patient data and have set penalties, both penal and financial, for noncompliance and breaches. For example, under the U.S. Health Information Technology for Economic and Clinical Health Act, hospitals and other organizations can be fined up to $1.5 million per year for serious security incidents. Corporate officers can also go to jail for negligence.

Intermountain, because of its scope, must follow health-related, banking and insurance regulations, all of which continue to evolve as cybersecurity gains importance. Evidence of this evolution can be seen in last year's audits by the U.S. Department of Health and Human Services' Office for Civil Rights (OCR). The OCR, which audits and enforces regulations from HIPAA and the HITECH Act, randomly audited 20 healthcare organizations; 19 failed, says Jiwani.

"We're finding the OCR has interpreted the regulations differently [from] industry," says Karl West, Intermountain Healthcare chief information security officer. "Because of this, we decided to innovate and partner with someone who could help us move into a new paradigm and a new interpretation of the regulations, and help us create a leadership position in the protection of patient information. That's how we came to work with CSC."

Segmenting networks and data encryption

A key area where CSC and Intermountain have teamed to set new benchmarks in the healthcare industry is a network approach that classifies data, encrypts data at rest and in transit, and then segments, or enclaves, data and systems — an approach that simultaneously protects data if stolen and protects data from being stolen. This approach, which CSC mainly uses in its public sector work, is a first for the healthcare industry, says Jiwani.

"Few organizations have looked at developing a strategy where they can encrypt and enclave their enterprise storage networks," he says. "We essentially took defense-level security and applied it to healthcare."

Under CSC's security work with Intermountain, CSC is helping the healthcare organization apply cutting-edge technologies and equipment from leading vendors that is mapped and embedded into these network design solutions.

Addressing BYOD, mobility and telemedicine

The network design principles encompass separation of duties and separation of data access. The design allows for managed and controlled access to containerized data based on need-to-know and access rights. They also include the use of approaches that support the confidentiality, integrity and availability of data through controls, and management around data access, data at rest and data transport across the network.

The end result provides Intermountain with a sound, scalable, self-healing, controlled and managed network infrastructure design that protects data, applications and systems containing electronic health information.

"This innovative approach, which balances a 'security everywhere' focus with one of 'security only where it's required,' allows us to be very agile and focus on those priorities that have the highest risk," says Jiwani. "We can dynamically change the areas where we want the most impact and resources, and use tools in a much more efficient way. It also allows us to determine the right level of risk versus cost."

While increasing security was already in Intermountain's five-year plan, because of rapidly escalating cyberthreats and evolving regulations, Intermountain decided to accelerate its security work. CSC helped the company leverage its discovery and monitoring tools to quickly and efficiently discover sensitive information without buying new technology. This effort, in turn, enabled the team to more quickly begin securing Intermountain's data.

"We normally see a program like this take three to four years to fully complete," says Jiwani. "Through some innovative approaches to programs, and using a new and differentiating approach to setting up this program, we have accelerated our timetable by 50 percent with less than half the budget we'd normally [devote] to this kind of project."

This kind of speed and network approach becomes increasingly critical, especially as physicians, patients, staff and visitors want to use their own devices to access Intermountain's systems.

"Every physician, every clinician has a favorite device, a favorite phone, a favorite mobile technology, and for us to keep ahead of those devices is challenging," says West. "We are working to develop strategies and technologies that enable them to safely and securely use these devices in their workflow and environment."

CSC is also helping the healthcare organization strengthen its administrative security controls, including updating existing policies, procedures and guidelines. With its extensive security training expertise, CSC is helping Intermountain develop a long-term training strategy and educational content that can be delivered through different forms of media to help its workforce better understand their security responsibilities.

"Our ability to help Intermountain Healthcare spans three key areas: people, processes and technology," says Jiwani. "We are bringing Intermountain an understanding of an industry-wide paradigm for security relevant to healthcare, while helping them understand the technology landscape and develop processes that are innovative and unique."

"I believe CSC is going to help us become a model healthcare system in the area of IS security," adds Probst. "We're not there today, but we have ground to move forward on. I'm very bullish on what we're creating together." ■

Ashif Jiwani, Partner, Healthcare Group, CSC

Intermountain Healthcare's Cybersecurity Challenge
Watch our Intermountain Healthcare Success Story Videos at csc.com/intermountain.

JENNY MANGELSDORF is a writer for CSC's digital marketing team.

NEW DATA BREACH RULES HAVE BIG IMPACT

by Richard Staynings

This January, the Department of Health and Human Services' Office of Civil Rights published the Omnibus Final Rule on amendments to the Health Insurance Portability and Accountability Act's Security Rule and the Health Information Technology for Economic and Clinical Health Act.

The rule makes significant changes to requirements involving security incident response and the notification of data breaches for HIPAA "covered entities," "business associates" and their subcontractors. Essentially it reverses the existing process, removes the "no harm, no foul" rule and requires CEs and BAs to conduct a comprehensive risk assessment to prove that no personal health information is compromised when a possible incident occurs. CEs and BAs are thus assumed guilty until they can prove themselves innocent — a fairly significant change in the fundamentals of U.S. law.

What's more notable is that the rule presumes that any unreasonable access, impermissible use or disclosure of PHI is a breach, irrespective of whether this caused, or was even likely to have caused, harm or damage to anyone. Thus if a nurse inadvertently sees the record of a patient not in her care, under the new rule, that action would constitute a breach and, at the very least, would require that a risk assessment be conducted.

These changes place a heavy burden on CEs and BAs' risk assessment resources and incident response teams, which need to rapidly investigate, document and report incidents as possible breaches to meet the new rule's requirements.

Other changes involve encryption, notices of privacy practices and breaches — even by organizations that do not have direct relationships with patients. The presumption is that organizations "know" collectively what their agents know and are liable for that knowledge as well as liable for acts or omissions of its business associates.

RICHARD STAYNINGS is a global cybersecurity and privacy officer, Healthcare, CSC.

Learn more at csc.com/cybersecurity.