TANIUM

Breaches and Supply Chain Risk Leaves Healthcare Industry Vulnerable

An eBook sharing best practices and guidance for Australian organisations to navigate through supply chain risks.

TANIUM

Connected Healthcare Vulnerabilities

The healthcare and life sciences industries have been embracing digitalisation to enable patient-centric care for some time. The timeline to completely move over to the connected-health approach has sped up since the pandemic to allow better patient outcomes and more effective and efficient healthcare by professionals and researchers. This eBook explores the challenges that connected-healthcare and supply chain poses for IT leaders.

Contents

How big is the problem in Australia?

The ability to collect data in real-time, together with the massive processing power of the cloud, provides the opportunity for dramatically improved decision making for the healthcare industry.

IDC predicts that by 2024," the proliferation of data will result in 60% of healthcare organisations' IT infrastructure to be built on a data platform that will use AI to improve process automation and decision making." But with all the benefits that connected healthcare, access to data, and new technologies bring, IT leaders are all too aware that there are inherent risks due to a combination of several areas. Three of these areas are:

Susceptible personal customer data: A survey of 230 healthcare security leaders in China, Germany, Japan, the UK, and the US ranked compromised customer data as their top concern as a result of a cyberattack (39%), followed by patient safety (20%) and stolen intellectual property (12%).

Critical services: The criticality of services delivered means the industry is more susceptible to threats holding them to ransom.

Supply Chains: Finally, there is considerable risk with supply chain vulnerabilities. Attackers look here as an easy entry point through medical devices, vendor technologies and software.

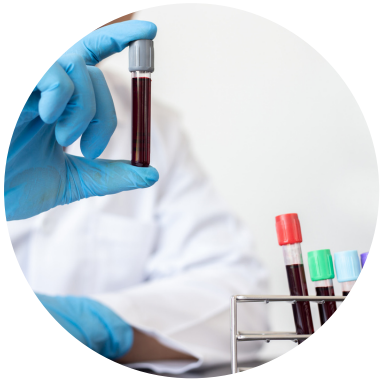
The growing threat in Australia

In recent years, attacks have increased exponentially. A survey of healthcare security leaders in China, Germany, Japan, the UK, and the US found that 82% of their healthcare organisations had experienced an IoT-focused cyberattack.

Ransomware has also grown in profile and impact, and it poses one of the most significant threats to Australian healthcare organisations. ACSC recorded a 15 per cent increase in ransomware cybercrime reports in the 2020–21 financial year. Prime Minister Scott Morrison also revealed a concerning wave of sophisticated cyber-attacks hitting critical infrastructure from all angles, including hospitals, local councils and state-owned utilities.

In the NTT Global Threat, Intelligence Report healthcare was reported to have experienced an increase in global attacks by 200% from 2019 to 2020. ACSC also reported the Australian health sector to have the second-highest number of ransomware incidents in 2020, right at a time when citizens were most reliant on this critical industry through the pandemic.

An example of the growing threat occurred in March 2021 in Australia. A ransomware incident affecting a Victorian public health service, which involved four hospitals and aged care homes, was reported to the ACSC. A Ryuk ransomware variant infected some of the health service's servers and workstations. The breach resulted in a partial IT system shutdown in the health service and postponed some elective surgeries.



What is a supply chain attack?

One of the biggest threats to the healthcare industry is an attack through the supply chain. These attacks occur when a cyber threat actor infiltrates a vendor or suppliers' network before inadvertently sending it to their healthcare customer. Organisations face growing challenges with more innovative, connected supply chains, carrying a flow of more intelligent, connected devices. They may simplify management and improve efficiency, but they also bring security risks in the world of the Internet of Medical Things (IoMT).

At the beginning of 2022, many organisations focused on responding to the Log4j vulnerability. The vulnerability affected hundreds of millions of devices around the world and was cast as a critical tech emergency that would almost certainly be exploited by attackers. Although after the Apache Software Foundation disclosed Log4Shell on December 9, the US Cybersecurity and Infrastructure Security Agency (CISA) said it hasn't seen a major breach arise from the attack, with the exception of an attack on the Belgian Defense Ministry. But CISA warned, that as Log4J is embedded in many applications, attackers might be lying dormant within a network and are waiting until alert levels fall to deploy malware months later.

It is a timely reminder for organisations to consider how to move from a reactive approach to address supply chain risk, to achieve a proactive approach.

Supply chain attacks leave healthcare vulnerable

Healthcare organisations are uniquely vulnerable to software supply chain attacks for two significant reasons. First, many third-party software products require privileged access; and second, many third-party software products require frequent communications between a vendor's network and the vendor's software product located on customer networks.

Even with these risks many organisations rely too much on blind trust and spreadsheets, manually assembled from a disconnected array of reports and data.

The challenge deepens for the industry when managing supply chains end to end. The complexity of modern supply chains can soon make risk management efforts spiral out of control. Many larger companies are exposed on multiple fronts. Many digital businesses use SaaS products, global data processors, hardware provided by third parties, outsourced software developers, and consultancy services. These third parties also use their third parties.

Healthcare organisations should ask themselves if they can vouch for the security practices of third parties. How many degrees of separation can they track? If the supplier in question had weak asset and application management processes in place, they might not even know the answer posed with any certainty. And what good is an assurance that’s based on partial or incomplete data?

Controlling of the external threat

Healthcare groups need to work directly with their vendors to reduce supply chain risks. They should consider requiring that every vendor, partner and supplier implements security controls to help minimise risks confronting their networks and products.

Tanium outlines the three areas of concern:

Security and risk teams engaged too late: Supply chain governance commonly happens too late in the onboarding process to leave enough time to mitigate or remove any risk that it discovers. The security and risk team can come under tremendous pressure from the business to bless the new deal. So they are not seen as the department that blocks innovation and progress to achieve the organisation's more significant goals. The chief information security officers (CISOs) may feel like they have no choice but to do so.

Recertification doesn't happen: As crucial and rigorous due diligence before onboarding is, a periodic reappraisal of the relationship is also critical. For example, you might use a SaaS provider whose service was initially deployed to just a small number of developers using only test data. That app may now be used by hundreds of employees and processing critical business information. Periodic recertification is vital to managing risk as it evolves dynamically. Unfortunately, it seems that supply chain security is "set and forget" for many organisations.

End-to-end visibility and assurance: Third-party risk management is one thing, but the further upstream or downstream you go, the harder it gets. What about the suppliers of your suppliers? The challenge here is that there's no consistent, industry-wide best practice for managing end-to-end supplier risk.

What should healthcare leaders do?

Although healthcare leaders are ready to increase spending on cybersecurity, with new threats uncovered every day, it isn't easy to know where an organisation would be better off investing their budget. High demand for patient information, outdated legacy systems, and too many disconnected tools, make the issue even more complex.

The answer is visibility

Organisations need to understand what IT assets they own, what's running on them, and what their third-party dependencies are. This sounds simple, but with 94 per cent of global IT executives and managers discovering endpoints within their IT environment that they were previously unaware of, it has been a challenge for many.

Suppliers must be subject to this exact requirement as well. Organisations must provide a comprehensive, accurate inventory of their IT assets to understand the status of endpoints and what software versions are installed.

And they must be able to patch promptly to mitigate risk dynamically. This inventory should be part of a holistic effort to calculate the overall maturity of suppliers' security posture such as — taking in partial point-in-time patch and vulnerability telemetry and a supplier's approach to threat modelling, secure software development, and their security architecture and much more. It isn't just about asking questions like 'do you run a particular version of software?'. The processes used to develop people and technology in a company are also critical. Focusing on prescriptive questions like, 'were you running the malicious SolarWinds Orion update?' assures leaders at a point in time but won't help when the next global cyberattack happens.

Questions every leader must ask

Adequate supply chain security demands a far more expansive approach. So what questions should leaders ask?:

- What is the meantime to deploy a critical patch?
- What percentage of endpoints don't conform to a CIS Benchmark Hardening Standard?
- What percentage of endpoints are missing the company's endpoint security tooling (AV, patch/vulnerability management agents)?

Once you have this quantitative data in hand, combine it with third-party attestation and evaluations to gain a 360-degree view of risk in each supplier.

Build protection into your processes

Consider some other ways to build up your supply chain protection:

- Involve security and risk teams early with the new supplier due diligence process.
- Perform periodic security certifications.
- Complete comprehensive threat modelling and risk analysis.

- Roll out transparent processes for breach notifications.
- Gather supplier approaches to secure software development lifecycle (SDLC).
- Define incident response playbooks.
- Request third party security policies that are refreshed annually.
- All vendors, suppliers and partners must maintain an evolving asset inventory. An accurate inventory list enables them to track new hardware and software and their owners, locations and configurations.
- Ask for evidence of a documented change management program that will enable them to respond to instances that might be signs of supply chain risks.
- Vendors must deploy the correct solution to harden their assets against supply chain risks, such as anti-malware solutions and vulnerability scanning tools.

Tanium for healthcare

Breaches are inevitable if organisations have endpoint devices connected to the public-facing internet. For healthcare organisations to stay ahead of adversaries and provide the best patient care possible, they need proactive, real-time and automated solutions and strategies. By reducing supply chain risk, increasing visibility across endpoints and finding, and then remediating vulnerabilities in the same console, organisations can avoid conflicting signals without priority indicators.

Using one console, security teams find threats faster, and operation teams avoid manual processes that cause errors and waste time fixing them. Today, incident response and forensics teams also recognise the need to collaborate more effectively to ensure that on-premises and remote endpoints are configured, controlled, and secured.

Tanium provides healthcare organisations access to reliable data in real-time. The search for indicators of compromise (IOCs) across an environment only takes seconds and allows organisations to know everything.

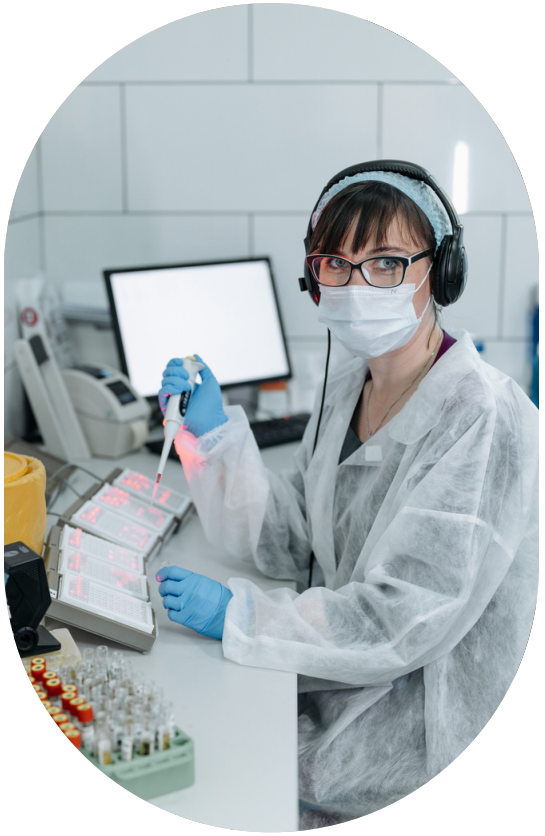
They can hunt for threats anywhere by isolating and remediating compromised endpoints without losing operator context or relying on fragile integrations. IT organisations can quickly investigate managed hosts for suspicious behaviour, with the lightweight Tanium agent used for operations and compliance. And finally, you can retrieve artifacts for your security operations centre and incident response teams, and scope lateral attack movement at scale will align teams.

Conclusion

The Cyber Security and Privacy Investigation Team at Sutter Health was pleased with their choice to deploy the Tanium Platform, "Tanium is very good at answering specific questions. Being able to get the data back is so satisfying and raises the level of quality of the analyst data."

Healthcare organisations around the world choose Tanium. It is an adaptive, scalable, and infinitely extensible platform for threat hunting, powered by accurate data to identify and proactively respond to threats in seconds.

Visit Tanium.com or request a demo today.



Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.
Visit us at www.tanium.com and follow us on LinkedIn and Twitter.