Healthcare cyber attacks: Lessons for Canada from Ireland's HSE attack

January 07, 2022

On Dec. 3, 2021, PricewaterhouseCoopers Ireland (PwC) reported on its independent review of the Ireland health sector's massive 2021 cyber attack.

In this article, we discuss the cyber attack, the report's findings and what Canada's public sector can learn from the attack and PwC's report. We also list six questions organizations should ask to prepare for and prevent such attacks.

Background

Overview of the attack and its impact

In May 2021, threat actors affiliated with the Conti group (Conti) deployed ransomware across Ireland's national healthcare network, a network operated by Ireland's Health Service Executive (HSE).

Conti provided the HSE with a useable decryption key (without HSE paying a ransom) soon after its attack, though the HSE's recovery process was still arduous and took a long time. The HSE restored 50 per cent of its network by just after mid June and the rest of its network by just after mid September.

The attack caused nationwide disruption to healthcare services. The HSE deferred some treatment and relied on private facilities, reverted to manual recordkeeping and faced significant additional patient safety risks. Employees, already stretched thin by the demands of working through COVID-19, had some payments delayed.

A vulnerable organization and network

The HSE is responsible for delivering health and social care services to all of Ireland's more than 5 million citizens and employs approximately 130,000 people. At the time of the attack, the HSE network featured 4,500 servers, 70,000 end user devices and more than 1,000 applications. The network spanned 4,000 physical locations.

The HSE delivers services based on a complex relationship with community health care organizations and hospital groups and in affiliation with “voluntary” hospitals who operate independently of the HSE. The entities with access to the HSE network shared what PwC calls a “bi-direction trust relationship” with the HSE, presumably in contrast to a relationship that put the HSE in stronger control.

By early 2021, the HSE identified its cyber risks and rated its maturity as low. It also understood its network to be “frail”: a “flat” (relatively unsegmented) network that had evolved over time to meet service-related needs, rather than the need for security and resilience. Heavy use of legacy technologies also burdened the network.

Staffing was also an issue: the HSE employed only 350 people in IT positions and only 15 in cybersecurity roles. The HSE drew its cybersecurity team heavily from IT personnel, and, according to PwC, the team lacked cybersecurity expertise.

How the attack happened

The attack dates to mid-March, when an HSE user clicked on a malicious Microsoft Excel document attached to a phishing email. The attacker then deployed known hacking tools on the user’s workstation and gained a foothold in the network. The HSE’s antivirus software detected the attack in late March, but was only set to monitor and therefore did not block malicious commands.

The perpetrators of the phishing attack may have sold this foothold to Conti, who re-accessed the network on May 7 and began to move laterally, in part by exploiting an unpatched and known vulnerability.

Various HSE entities saw indications of compromise between May 7 and 14, when Conti deployed its ransomware. One independent hospital and the Department of Health seized upon alerts and successfully blocked the deployment by forcing password resets, reconfiguring firewalls and using protective security tools. The HSE itself did not mobilize fast enough, in part because it misinterpreted the evidence as suggesting the independent hospital was the origin of the threat. PwC attributed this failure to the size and lack of expertise of the HSE’s cybersecurity team.

The recovery effort

The HSE had not planned for such an incident, and according to PwC, suffered because of the following deficiencies:

- No cybersecurity response plans or playbooks;
- No security tooling capable of investigating and remediating security alerts;
- No centralized list of contact details for all HSE staff or an asset register;
- No offline copies of key IT security and documentation;
- No pre-established prioritized list of applications and system for recovery, in particular a list cognisant of cross-technology dependencies; and
- No pre-agreed, set up and tested out-of-band communication system.

As a result, the HSE spent time in its recovery effort gathering information about its network and needed to re-prioritize and adjust as it proceeded. The lack of

documentation and resourcing placed a heavy burden on key personnel, causing "bottlenecks" and slowing down the HSE's recovery.

There also appears to have been some fragmentation in legal positioning: one independent hospital whose data Conti published on the dark web, together with HSE data, decided to notify affected data subjects. The HSE decided notification was unwarranted because the personal data risk to the rights and freedoms of individuals was too low.

PwC's findings and recommendations

PwC made a number of findings in its 100-page report, and focused on the need for transformational change. Based on these findings, it made four strategic recommendations:

1. Implement an enhanced governance structure over IT and cybersecurity that will provide appropriate focus, attention and oversight. Between the HSE and the entities who participate in the HSE network, PwC recommended that the HSE take control, including by developing and enforcing a "code of connection." Internally, PwC recommended that the HSE establish executive level cybersecurity and IT committees and a board committee (supported by outside experts) to oversee the required change to the HSE security program.

2. Establish a transformational Chief Technology & Transformation Officer (CTTO) and office to create a vision and architecture for a resilient and future-fit technology capability; to lead the delivery of the significant transformation programme that is required, and to build the increased function that will be necessary to execute such a scale of IT change. According to PwC, the HSE's current chief information officer lacks the mandate, authority and budget to conceive of and build a more resilient HSE network. It envisions a CTTO who will develop a new strategy, one that warrants significant incremental funding.

3. Appoint a Chief Information Security Officer (CISO) and establish a suitably resourced and skilled cybersecurity function. Develop and drive the implementation of a cybersecurity transformation program. PwC said the HSE needs a CISO to drive organizational change, stating that "The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the [Executive Management Team] and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making."

4. Implement a clinical and services continuity transformation program reporting to the National Director for Governance and Risk, and enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT. Although it recognized service continuity as an HSE strength, PwC nonetheless recommended change in order to establish service continuity as a risk discipline and co-ordinate processes across the organization.

Takeaways

1. The Ireland cyberattack illustrates the perils of IT and security governance models that do not clearly assign accountability and authority to a single entity. Many parts of the public sector have adopted complex shared IT services models that may lack resilience because accountabilities and authority are unclear or shared between entities.

Ask: Do you have a strong enough governance model?

2. The Ireland cyber attack illustrates the need for proactive incident response planning and, for complex IT systems, provides helpful guidance on planning focus. According to the PwC, even though the HSE had exceptional crises management and emergency response skills, it was impeded by a lack of planning. The PwC report focused strongly on asset mapping, prioritizing services and systems for recovery, and identifying dependencies between services and systems.

Ask: Do you have an up-to-date network map and inventory of systems that addresses prioritization and dependencies?

Ask: Do you have an incident response plan that identifies roles, responsibilities and key tasks?

3. By engaging PwC to conduct an independent review of its cyber attack, the HSE will benefit from PwC's strong remedial analysis. The root cause of the Ireland attack was not human error that led the HSE user to fall for a phishing scheme. Rather, the cause was an organizational problem that prevented the HSE from building a resilient network and responding optimally to the cyber attack. Not every incident will warrant the depth of probing invited by the HSE. However, organizations that suffer attacks without robustly analyzing what happened and why will remain vulnerable.

Ask: Do you have a user awareness program that adequately addresses the risk of phishing, consistently one of the top attacks used by threat actors?

Ask: Does your incident response plan commit to causal analysis that will lead you to address immediate and root causes?

4. The Ireland cyberattack highlights that cybersecurity, particularly in the public sector, is a matter of strategy, funding and organizational change. The HSE was operating critical public infrastructure, faced critical risk and had rated itself as having low cybersecurity maturity. This concerning state of affairs was apparent to the HSE, but it did not change fast enough to protect itself and the public that it served. Many Canadian public sector entities are on the same "burning platform" the HSE was. Their challenge is to transform themselves – ideally before, rather than after, suffering a major incident.

Ask: What can be done to initiate lasting change and foster better government support before suffering a major cyber attack?

Ask: How can you leverage your causal analysis, either together or with other organizations, to make a case for better government funding?

Is your organization at risk from the same governance and incident response weaknesses that made Ireland's HSE vulnerable? If so, now is the right time to ask

questions and seek assistance, and any of the authors of this article are available to provide support.

By

Eric S. Charleston, Daniel J. Michaluk

Expertise

Cybersecurity, Privacy & Data Protection, Health Law

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749