Between 27 June to 4 July 2018, SingHealth, Singapore’s largest group of healthcare institutions, was victim to the worst cyberattack in the country’s history, with a data breach of 1.5 million patients. Impending hearings are set to commence 28 August 2018.

Gino Bello, Senior Director of Technology in Singapore, sat down with FTI Consulting’s Global Head of Cybersecurity, Anthony J. Ferrante (previously Chief of Staff of the FBI’s Cyber Division and Director for Cyber Incident Response at the U.S. National Security Council at the White House), to discuss what can be learnt from the attack and how companies can protect themselves.

Gino: Anthony, thank you for your time. A number of weeks ago, Singapore experienced the country’s worst ever data breach, with personal information being stolen from SingHealth’s computer systems, including Prime Minister Lee Hsien Loong’s information. A four-member Committee of Inquiry (COI) has been set up to investigate the cyber attack, with hearings expected to commence in the coming weeks, but do we know who could have done this? And why?

Anthony: Reports have indicated that this sophisticated cyberattack was a state-sponsored effort specifically targeting the information of Prime Minister Lee Hsien Loong. Cyber-criminal tools like malware are increasingly being leveraged by nation-states seeking inexpensive – and easily deniable – ways to conduct targeted operations. Geopolitical tensions can lead to incidents like this, particularly as nation-state actors become more equipped to launch attacks on this new frontier of cyberwarfare.
As we continue to connect more and more of our infrastructure to the Internet, we create more entry points for attackers. Businesses should be continually assessing and upgrading their cybersecurity measures, conducting vulnerability assessments with third-parties such as FTI Consulting to find gaps and implement strategies to consistently and effectively protect their most critical assets.

**Gino:** Names, Identity Card (IC) numbers, addresses, gender, race and dates of birth have been taken. In our experience, when coupled with credit card numbers, phone numbers and email addresses, we have seen victims of identity theft as well as insurance and health claims fraud. With such profitable information being taken, what else could it be used for?

**Anthony:** Cyber criminals are primarily motivated by monetary gains and pose a serious threat to corporations. They are often laser-focused on stealing personal data so they can sell it on the black market to identity thieves. Cyber hacks may seem improbable, or even unlikely, but they often have a severe impact on operations, consumer trust and even, financial standing. While the attack on SingHealth has not led to the disruption of health care services, we have seen other breaches – like the ransomware on the United Kingdom’s National Health Service (NHS) – have a large-scale impact on a hospital’s operations.

**Gino:** In 2017, Singapore led the International Telecommunication Union’s (ITU) Global Cybersecurity Index (GCI) rankings and has invested significantly in cyber defenses through its specially formed agencies and committees, including the Cyber Security Agency of Singapore (CSA) and the Personal Data Protection Commission (PDPC). In February 2018, Singapore passed a Cybersecurity bill, establishing a legal framework for the oversight and maintenance of national cybersecurity in Singapore. In the incident with SingHealth, the government acted swiftly, promptly disclosing the attack and deploying an effective incident response plan and launching a Committee of Inquiry. What can countries learn from Singapore’s reaction? Are there other examples where cyberattacks have not been contained so effectively and what have the implications been?

**Anthony:** It is critical for companies to understand their cyber risk profile, or how an attack or breach could affect their business, and to use that information to inform a cyber incident response plan. Business leaders should ensure that their organisation has protocols in place that will help them to identify the source of and contain the incident, and a plan for disclosing the scope and scale of the incident to relevant stakeholders (customers, regulators, employees, partners, vendors, etc.).

One case study that we often consider when helping companies mitigate cyber risks is the ransomware attack on the National Health Service (NHS). The global ransomware attack on the UK’s publicly-funded NHS blocked access to patient records, schedules, phone lines and emails, proving highly disruptive for patients, doctors and emergency medical services personnel. This attack demonstrates the importance of strong cybersecurity measures for healthcare services, and why companies across all industries need to have a robust cybersecurity incident response plan. Now, as the NHS works to upgrade its cybersecurity system, policies, and training, it must also work towards restoring the public’s trust in a national healthcare institution – a far greater challenge than they may have anticipated.

**Gino:** You’ve seen many attacks from your experience with the FBI, the White House, and now leading FTI Consulting’s Global Cybersecurity team. What are you seeing globally with other cyberattacks and the level of sophistication that the hackers have reached? At a global level, what is being done to tackle cyber threats? What can companies in Singapore and the region take on board?

**Anthony:** As we continue to connect more and more of our infrastructure to the Internet, we create more entry points for attackers. There are a variety of malicious cyber actors that also pose a significant threat to corporations, and these hackers are becoming increasingly advanced every day, finding ways to circumvent the most state-of-the-art protections. Indeed, there is no perfect cybersecurity incident prevention plan – in fact, there is no way to prevent an attack on your organisation. However, there are many best practices that companies proactively adopt across industries to reduce the risk of a cyberattack. This may include implementing – and enforcing – policies and procedures, making sure vendors have secured their data, and creating a “culture of security” whereby employees understand their role in prevent cyber incidents. Most importantly, businesses should be continually assessing and upgrading their cybersecurity measures, conducting vulnerability assessments with third-parties such as FTI Consulting to find gaps and implement strategies to consistently and effectively protect their most critical assets.

**Gino:** Finally, Anthony, what can individuals do to better protect themselves?

**Anthony:** Personal information can be very valuable to malicious hackers, making us all attractive targets. Each and every one of us needs to be vigilant to catch the exploitation of personal information resulting from a cyberattack. I recommend using credit and identity monitoring services to catch any suspicious activity and stop fraud in its tracks before it’s too late.
FTI Consulting’s cybersecurity business build a safer future by helping organisations understand their own environments, harden their defenses, rapidly and precisely hunt threats, holistically respond to crises, and sustainably recover their operations and reputation after an incident. Led by Anthony J. Ferrante, previously Chief of Staff of the FBI’s Cyber Division and Director for Cyber Incident Response at the U.S. National Security Council at the White House, our seasoned experts bring unparalleled technical and practical experience to the delivery of cybersecurity solutions.

**OUR CYBERSECURITY CAPABILITIES & OFFERINGS**
Comprehensive services to organisations to manage and protect from Cybersecurity challenges

**ASSESS and Understand Your Environment:**
Managing cybersecurity risk begins with developing an organisational understanding of your business environment and its assets. We conduct assessments that inform the development of strategies to manage and mitigate cybersecurity risk to your systems, assets, data, and capabilities.

**DEFEND Your Assets and Infrastructure:**
The deployment of network safeguards is critical. We identify, implement, and manage defensive best-practice processes including access control, awareness and training, data protection policies, network maintenance, and deployment of protective technologies. Through these defensive measures, we ensure the delivery of your critical services and operations.

**IDENTIFY Threats Rapidly and Proactively:**
Timely discovery of impacts to your network can be a key factor in minimising damage. By implementing continuous security monitoring and advanced detection processes on your networks, FTI Consulting experts can detect anomalies and other security-related events rapidly and proactively.

**RESPOND to an Incident Holistically:**
Once you detect a cybersecurity incident, you must take action. We provide complete cyber incident response options that include planning, analysis, mitigation, system refinements, and ancillary mission support functions, such as strategic communications and reputation management.

**RECOVER Operations Quickly and Sustainably:**
Restoring capabilities or services that have been impaired is often your top priority when you face a cybersecurity incident. We develop recovery plans that ensure long-term improvement, limit the potential lasting impacts of cyber incidents, and prevent damage from future incidents. With our recovery assistance, you can get back to business as usual, as soon as possible.

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

For more information, or to discuss your organisation’s cybersecurity defenses, please contact:

**Washington, DC**
Anthony J. Ferrante
Senior Managing Director
Global Head of Cybersecurity
+1 202 312 9165
ajf@fticonsulting.com

**India**
Amit Jaju
Senior Managing Director
+91 022 5036 5016
amit.jaju@fticonsulting.com

**Singapore**
Gino Bello
Senior Director
+65 6831 7856
gino.bello@fticonsulting.com

**Hong Kong**
Sandeep Jadav
Managing Director
+852 3768 4730
sandeep.jadav@fticonsulting.com

**About FTI Consulting**
FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

www.fticonsulting.com