HIMSS

Protecting digital health systems and patient information:

Five key takeaways from a HIMSS APAC Cybersecurity and Privacy Government Virtual Roundtable

Overview

Healthcare throughout the Asia-Pacific (APAC) region has transformed rapidly during the pandemic as digital technologies have been integrated, even in countries that had previously relied on paper-based systems. But with digital systems comes great responsibility to ensure that data collected remains safe.

For most people, health information is the most confidential piece of information in their lives. Meanwhile, the work of healthcare organisations is among the most vital of all critical infrastructure sectors. Health data needs to remain private while healthcare providers need to be able to operate without disruptions, which is why cybersecurity and privacy are priorities for all health systems.

A HIMSS priority is ensuring the security and privacy of patient health information globally, which is why a collection of nations was brought together for the APAC Cybersecurity and Privacy Government Virtual Roundtable.

Eli Fleet, director of government relations at HIMSS, outlined the HIMSS vision: "We're working towards the development of a unified global approach to health cybersecurity information. We don't want a one country, one approach. We think that cybersecurity is a topic that is borderless."

HIMSS believes this can be achieved through the creation and adoption of voluntary consensus-based industry led guidelines, best practices, methodologies, procedures, and processes, with use cases and implementation guidance.

From a policy perspective, HIMSS ensures that recommendations and resources to governments relating to cybersecurity are scalable for a wide range of healthcare organisations – from small practices to large health systems.

Context

HIMSS presented a set of cybersecurity and privacy policy recommendations at a virtual roundtable held on 24 February 2022. This discussion was attended by government representatives from seven APAC countries: Bhutan, Hong Kong, Japan, Malaysia, Singapore, Pakistan and the Philippines. A representative from the World Health Organization was also present. As the roundtable was held under the Chatham House Rule, the participants quoted in this report have been de-identified.

Moderators:

Eli Fleet
Director, Government Relations, HIMSS

Lee Kim
Senior Principal, Cybersecurity and Privacy, HIMSS

Ashley Delosh
Senior Manager, Government Relations, HIMSS

Key Takeaway 1:

Strength in numbers to safeguard systems

Cooperating on cybersecurity through "coalitions of the willing", including across national borders, is effective in bringing about legislation and counteracting cyber attackers.

"One of the biggest things around cybersecurity that HIMSS has really worked on over the last number of years has been around building coalitions in cybersecurity," Fleet said. "This is not a healthcare only issue. This is an issue that touches on all parts of society and so we need a 'coalition of the willing'. "

In the United States (US), the Chamber of Commerce has led a cyber coalition that HIMSS has been a part of for almost seven years.

According to Fleet, cyber attacks in the last year or so have led to a discussion on how organisations are notifying the federal government agencies and law enforcement when an attack occurs. Efforts were made to legislate notification requirements, but it was not enacted into law. HIMSS is hopeful that at some point in 2022, in a number of legislative vehicles, it might become a legal requirement.

"[For] the government to be able to respond to cyber attacks – not just at the healthcare level, but across all sectors – it's critical for them to know when they happen and when ransomware is paid out," Fleet said.

The proposed legislation would require notification of a cyber attack to law enforcement within 72 hours, or within 24 hours of a ransom being paid.

In terms of healthcare, in 2015 HIMSS led a coalition advocating for healthcare provisions in the Cybersecurity Act. It required the creation of a task force of industry leaders who assessed the challenges and cyber threats. They then made recommendations to the Department of Health and Human Services in its Healthcare Industry Cybersecurity Task Group Report, which was released in 2017. The report recommended the Department of Health and Human Services create a series of best practices for the healthcare industry to follow, on a voluntary basis, to help keep their organisations' data secure.

This effort has evolved into the 405(d) Task Group, which raises awareness, shares vetted cybersecurity practices, and moves organisations toward mitigating the current, most pertinent cybersecurity threats. "The idea behind this task group is to provide resources for the healthcare sector that are not just critical and understandable to the CISO or to the cybersecurity technical experts, but to anybody in a health system who opens an email that could contain a threat," Fleet said.

In 2019, they released the Healthcare Industry Cybersecurity Practices (HICP) document, which outlines base level cybersecurity practices that organisations can implement and build on. They have also produced free resources for people of all technical capabilities to easily understand, available via a government website which is constantly being updated. HIMSS has been involved in this effort.

In the US, there is also a Healthcare and Public Health Sector Coordinating Group, which contains a Cyber Security Working Group that currently has over 300 members. It is made up of associations, such as HIMSS, as well as various healthcare systems and industry, including medical device and pharma companies. The idea is to work together to monitor and create guidance around cybersecurity practices. As the US is not the only nation stepping up its cybersecurity, the working group has had presentations over the last couple years on what is happening in cybersecurity practice in New Zealand, Australia, Israel and others.

In Japan, a serious cyber attack has spurred health systems and providers to form a private coalition of health entities to focus on improving cyber defenses. "Right now in Japan, we don't have a good legal structure for cybersecurity. However, last year, one hospital had a severe attack involving ransomware. And that hospital's operations were affected. So looking at that issue, we are now thinking of doing a project on this. We are now trying to start some kind of a [private] consortium with medical device companies and hospitals, so we can handle and share information about these kinds of issues," they said.

A participant from Pakistan said it's important for nations to share their wisdom and collectively work to achieve cyber secure systems: "I feel with these forums that HIMSS has [organised], countries can share about what they're doing. And we can learn from [these] experiences and adopt those recommendations or guidelines, rather than just creating a lot of things from scratch."

Key Takeaway 2:

A shifting privacy landscape as innovation oustrips legislation

The complicated privacy "patchwork" of obligations places pressure on healthcare as legislators struggle to keep pace with innovation.

HIMSS is continually involved in privacy-related responses to the US government through multiple different federal agencies. Ashley Delosh, senior manager of government relations at HIMSS, said the priority is to emphasise patient right of access and control of their own healthcare data and information.

The major federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), is the overriding legislative mechanism. But as new regulations at the state level come about, there is a patchwork effect that HIMSS helps its members to navigate.

Extending beyond healthcare, there are numerous consumer privacy rights that also have implications, specifically to third party applications.

"The privacy discussion is ongoing and we're trying to stay on top of it, but it is a beast to get our heads around. We always try to emphasise alignment with new regulations and existing ones that are being updated to keep pace with technology, even though it is really complicated as the speed of innovation is much faster than our federal government," Delosh said.

The slow pace of progress in terms of privacy legislation in Congress means the states can have the inside running. "There's been a hold up in Congress [and] privacy has taken a bit of a backseat," Delosh said. "There are conversations about a comprehensive healthcare privacy law on Capitol Hill in Washington, but nothing set in stone. So it's something that we continuously monitor because we're continuing to see states come up with their ideas on privacy laws. Most recently Colorado and Virginia, and California has one that sets the tone."

HIMSS is engaged in shifting the conversation to a more global focus given that privacy touches everyone's lives, particularly in healthcare.

In the Philippines, the Department of Information and Communications Technology is the national government agency mandated to ensure the protection of individual privacy rights and the security of critical ICT infrastructure, including information assets of the government. A national cybersecurity plan and Data Privacy Act are in place.

"Operationally, in the health sector, we have embedded data privacy and cybersecurity measures as part of the minimum requirements in implementation and maintenance of our integrated health information systems and telemedicine services," a participant from that nation told the roundtable.

"So right now we have issued policies institutionalising the adoption of these requirements in our health facilities and other health related entities that are implementing or processing health information, and at the same time for other sectors. The implementation is already underway, and we hope that in the near future we will be able to fully implement it across the Philippines."

Key Takeaway 3:

Gone phishing: human factors impacting cybersecurity

Critical infrastructure organisations such as healthcare providers remain blue chip cyber targets with greed continuing to exploit human error.

The electronic environment we live in – in which we receive, store, transmit and create electronic information – means that cybersecurity applies to all of us. The 2021 HIMSS Healthcare Cybersecurity Survey and learnings from industries across sectors show that critical infrastructure sectors, which are the sectors that societies need to function, such as healthcare, finance/banking, water or gas supplies, are targets for cyber attack.

Meanwhile, healthcare is one of the few sectors that depends on almost all other sectors to operate effectively. In addition, patient safety is paramount, raising the stakes as to why cybersecurity is critical.

"That said, we have been monitoring what attackers are after in terms of assets and such, and we found that for the second year in a row financial information is still, by and large, the main target. Why? That's, of course, where the money is," Lee Kim, senior principal of cybersecurity and privacy at HIMSS said. "So that's still the name of the game for cyber attackers of all types and stripes. These can include nation state actors, non-state actors, cyber criminals, amateur hackers, whomever. Money is still king, as we all know."

Attackers by and large are getting into systems via phishing, Kim said, describing it as "essentially the golden ticket inside" IT systems. "You might ask why? The reason why is because we are behind the fire walls. If someone is able to fool us into opening an email, giving up sensitive information, and/or clicking on a poison link or malicious attachment, they've essentially bypassed the need to break into systems from the outside, such as getting past firewall defences, cracking passwords, etc, by simply sending us an email," Kim said.

A participant from Hong Kong said that due to COVID-19, more colleagues are working from home, making it even more challenging to raise awareness of cyber attacks and how to be vigilant.

"Phishing is always the entry point. It's something we do focus on in terms of how to create more effective situational awareness. We already try to do some phishing exercises and we treat this like a test, but we really need an exercise to make the users feel and experience how real the attack is," they said.

"Because in most cases in healthcare, they care most about serving the patient, providing clinical services. And IT is just a tool for them. So it's sometimes very hard, it's not easy to educate them that the bad guys are targeting you. So I think this is a culture shift and how to make this happen, I think is not purely for IT or even CISO to do. I think it really requires more collaborative behaviour changes."

In Malaysia, phishing is a huge ongoing threat but only a few hospitals use an electronic medical system, most of which are on premise. The country's representative explained: "So we have not really had real attacks or data leaks happen so far as we have employed very strong passive measures against attacks from outside from the external internet. But moving forward as we move towards account based and maybe a web-based sort of access and health information system, we are looking towards strengthening cybersecurity as far as the access goes," they said.

"But we also do struggle with budget, especially in terms of having more active participants toward these cyber attacks from the outside. We do occasionally get DDoS attacks. But so far nothing valuable has been stolen really. Just maybe disruption to the service which we've managed to handle without much fuss."

Key Takeaway 4:

Continual threat requires constant defence

The consequences of disruptions to healthcare services can be dire for patient care, which means maintaining cyber defences requires blocking and tackling of intrusions – fast.

The roundtable heard that the typical impact of cyber attacks is disruption – whether it be to business operations or clinical operations – rather than damage to systems or the wiping of data. Disruption is a particularly important impact in healthcare given that it can lead to delays in patient care and significant differences in terms of patient outcomes.

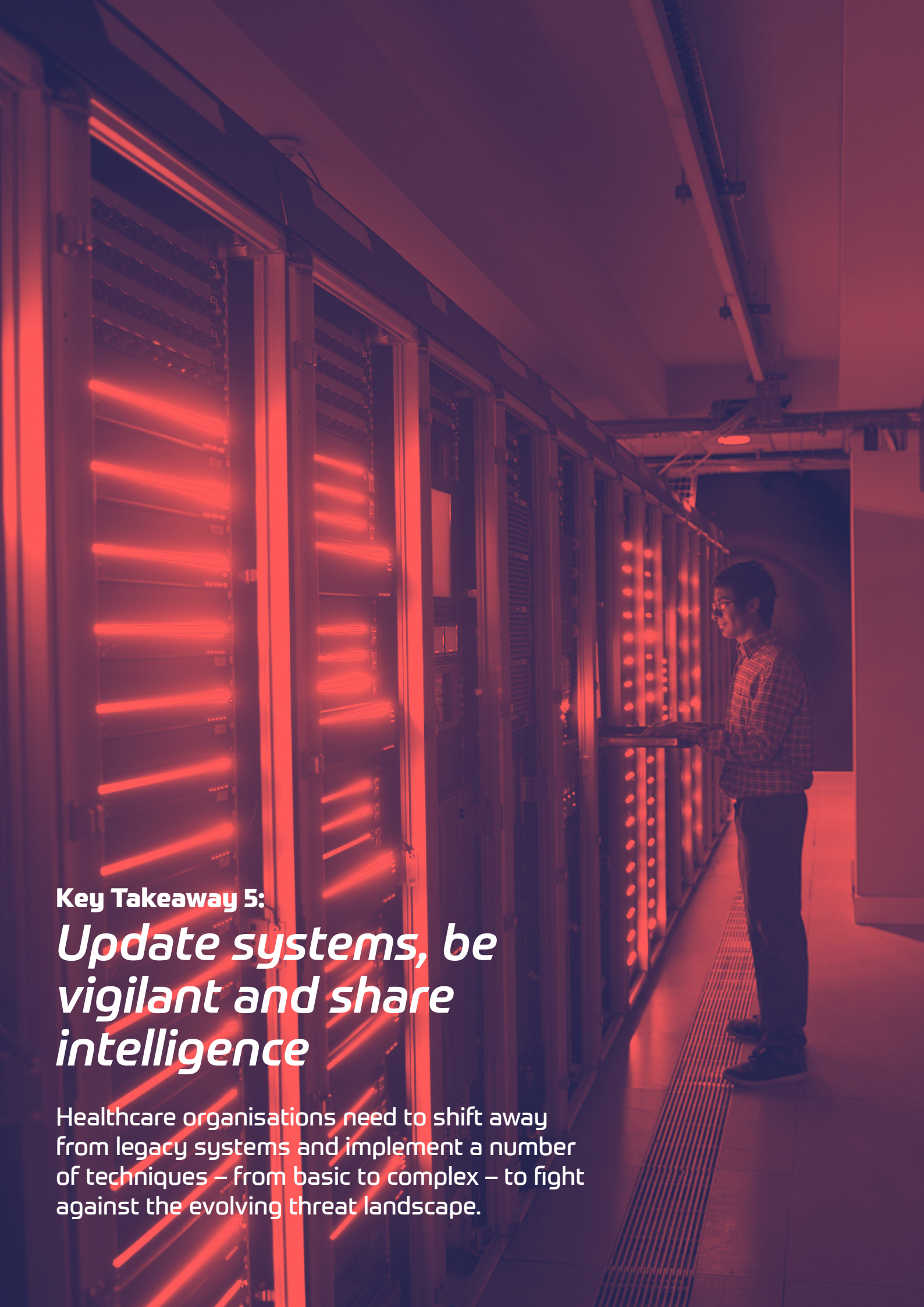
Even still, regardless of the country or the kind of hospital organisation – public or private – budgets remain by and large very tight. It means that cyber security professionals may know exactly what they need to invest in to have a complete complement of basic and advanced security controls. But unfortunately, budget limitations may lead to the implementation of a few security solutions that can be upgraded, rather than the full suite needed to provide the best defence.

Typically, cyber criminals are extremely skilled and scour systems looking for one mistake that has been made in terms of configurations. As a result, health IT infrastructure needs to be impenetrable all of the time to absolutely prevent breaches and other compromises. But there is no 100 per cent, perfect performance in terms of cyber defence in the real world. That's why it requires the blocking and tackling of cyber intrusions as soon as possible in order to stop "the bleed of data" and other compromises.

A participant from Bhutan told the group that the nation's healthcare sector had turned to digital systems during the pandemic and now needed to gain greater awareness of how to keep data safe.

"In terms of information technology, digitising and all that, I think Bhutan is behind many countries. But for the Ministry of Health in Bhutan during COVID-19, many things went digital. We had a Bhutan vaccine system, which required all data to be digitised. We also initiated other digital recordings for quarantine isolation. Also, we are now rolling out an electronic personal information system nationwide. So this provides an opportunity [for us to] be more aware of cybersecurity and [privacy]," they said.

They added that a take-home message from the roundtable was that even though the Ministry of Information and Communication is responsible for cybersecurity, at the Ministry of Health level the Health Bill is currently being drafted, providing an opportunity to add clauses addressing cybersecurity needs. A working group for cybersecurity should also be created to work with the eHealth Steering Committee.



Key Takeaway 5:

Update systems, be vigilant and share intelligence

Healthcare organisations need to shift away from legacy systems and implement a number of techniques – from basic to complex – to fight against the evolving threat landscape.

Many healthcare organisations worldwide use legacy technology systems, with Windows remaining dominant. According to Kim, while operating systems are being "sunsetted" every several years, healthcare organisations are not planning for obsolescence. As a result, cyber attackers have stockpiled hundreds of exploits against legacy operating systems.

The United States Department of Homeland Security's cybersecurity agency, the Cybersecurity and Infrastructure Security Agency (CISA), produces a bulletin containing the most common vulnerabilities. Kim advised participants to consistently review their systems against the malicious codes listed and patch against them.

"Unfortunately, many organisations are not vigilant enough and forgo immediate patching. But time is of the essence because once a vulnerability is announced, cyber attackers need to exploit as many systems as they can before patches are released and applied. That is why it is critical for healthcare organisations to have a robust and regimented vulnerability scanning and patch management program," she said.

Additionally, across healthcare organisations of all sizes and types, there can be gaps in the use of simple repellents such as antivirus applications and firewalls, while the majority of healthcare organisations are not implementing encrypting solutions. Otherwise, encryption solutions that are frequently used provide very weak protection. Kim said that as an industry healthcare needs to take a stand and use much more robust encryption in place and demand that internet service providers also deploy much stronger encryption than currently evident.

HIMSS has also found that many healthcare organisations are unaware of bug bounty programs or at least they aren't participating in them, which is a lost opportunity to test a specific portion of their environment to see what vulnerabilities may exist that may be readily exploited. Bug bounty programs provide a crowdsourced mechanism whereby the very best security researchers can test systems and determine any breaking points, allowing organisations to close the gaps and upgrade security solutions or operating systems.

Finally, Kim urges the sharing of threat information between countries because "there's very little that's more valuable than intelligence".