IIJ and the Evolution of Security —Commemorating 30 Years

3.1 Introduction

All sorts of incidents and accidents have occurred since we started our security business. Looking back on the past 30 years, the Internet has established itself as a platform for one-to-many and many-to-many communications in a communication services world that had primarily been a one-to-one affair. And those communications are always changing, both in form and composition. It started out as a network that only some people used, but those times have changed with the advent of commercial services for business customers and the like, consumer services, always-on connections for the home, mobile phone-based access, the cloud, smartphones, and IoT technologies.

The way we use it has also changed, and this has changed our everyday lives. In particular, with browser-based encrypted communications having become standard, electronic commerce has thrived, and the addition of personal authentication and other such features means we are now able to exchange vital, financially valuable information on a routine basis. Making credit card purchases and logging into online banking via your smartphone is the norm these days.

Yet this situation works in a similar vein for malicious actors too, who are able to exploit the nature of Internet communications to send data out over large distances to many recipients at low cost. Because the transmission of these communications takes place between computer systems, malicious actors are also able to exploit vulnerabilities to wreak havoc before users even realize what is happening. And the spectrum of malicious activities is broad, ranging from simply hijacking and using systems without permission to the theft of valuable information and services, the theft of intellectual property, ransom demands, and more.

In this article, a number of people who have worked on the front lines of IIJ's security business share their experiences and give their own unique perspectives on the past 30 years.

The Changing Face of Network Threats

Hirohide Tsuchiya
Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Divisionn

Commercial Internet arrived in Japan in 1993, and worms, viruses, and other such threats have also been with us since. Attempts to log in to open ports and other such behaviors were also part of the landscape. Given that companies need to guard against such attacks when using the Internet for business purposes, IIJ launched Japan's first firewall service back in 1994.

Initially, the Internet was generally used simply to pass information around; people were mostly browsing homepages or sending emails and messages. Once the year 2000 rolled around, the Internet started to transcend this and serve as a form of social infrastructure for business and other economic activities, including financial services and online shopping, leading to a rapid rise in prominence. This also prompted more awareness of the importance of security, and a recognition of the importance of security defense measures and the need to address vulnerabilities. Individuals were encouraged to use antivirus software, and companies also deployed security products such as firewalls and IDS/IPS on top of this.

Security incidents also became more diverse, with cases of website tampering, website DDoS attacks, and network worm infections via the Internet occuring quite frequently and being reported in the press. The typical network worm infections included CodeRed and Nimda, which reared their heads in 2001, and SQL Slammer, which popped up in 2003. Once these worms gained a foothold, the infections spread around the globe blindingly fast, in some cases resulting in network latency and other impacts. While Internet usage was growing rapidly, communications lines and other equipment were not as abundant back then as they are now, and our means of responding to large-scale

attacks like this were limited. Today, our communications infrastructure and attack countermeasures are more fully developed, but with the spread of IoT devices and the like, the volume of data traffic associated with attacks is now several hundred times what it was back then.

As time passed, attack methods became increasingly complex and sophisticated, evolving to include botnets, which exploit vulnerabilities to infect and take control of large numbers of devices, like PCs and routers, to carry out DDoS attacks; malware (malicious computer programs) that steals user information and other data; and ransomware, which encrypts data on infected devices, effectively taking it hostage, so that the attacker can demand a ransom. Systems for carrying out these attacks were developed like any other software and made available on underground markets, such as the dark web, making it possible for anyone with a little money to obtain the tools to launch an attack in pursuit of ill-gotten gains.

As security countermeasures advanced and made it difficult to attack networks directly, the attack methods again morphed in clever ways, instead seeking to infect systems via email or by directing users to malicious links, and so forth.

Even today, infection campaigns that attack networks indiscriminately are still carried out, but attacks in general have become more advanced and include those directed at a narrow range of targets to make the infection campaign more efficient as well as targeted attacks and APT attacks, which seek to fly under the radar so as to evade detection and avoid triggering a security response.

With the Internet having come to serve as a form of social infrastructure, changes in the value of computing resources and information have elicited changes in the purpose of attacks as well. There was a time when some unknown number of faceless individuals out there were carrying out attacks partly for the fun of it, but attacks now serve a range of different agendas. Hacktivist groups like Anonymous, for instance, have carried out protests designed to publicize certain ideologies or claims, we now see financially motivated attacks being carried out by individuals and groups, and certain organizations and countries now engage in efforts to steal information.

These sorts of activities have also now gained the ability to impact on the real world when used in conjunction with methods outside of direct network attacks, such as the spread of false information, “fake” news, and the like on social media and, in some cases, public demonstrations or even terrorist acts.

This increasing sophistication and changing nature of attacks means that it is no longer enough to monitor what’s happening within and on the boundaries of a network to protect information in the hopes of preventing an attack. And as such, new security frameworks are being implemented in the form of zero trust models and the like to provide constant access control and monitoring of people, assets, and data.

If we consider the situation in terms of attackers and defenders, the attackers do seem to have a persistent advantage in many cases. If we are to break this paradigm, we need not only technological solutions but financial and legal countermeasures that diminish the advantage to attackers as well. As the Internet evolves, Japan has been updating its legal system where necessary, establishing the Act on Prohibition of Unauthorized Computer Access, for instance, and adding provisions to its penal code to explicitly criminalize the use of “electronic or magnetic records containing unauthorized commands” (in other words, computer viruses). Yet the Internet is truly borderless, and as such, many issues need to be considered in a multinational or even a global context. Many initiatives and cooperative international efforts have been mounted in all sorts of areas to address these issues we face, but we will need to join forces to an even greater extent going forward.

The range of communication modes available also continues to diversify to serve individual use cases—the reciprocal use of microcells and mobile networks, for example, and satellite-based connectivity services. And as connectivity continues to permeate our everyday conveniences, cars being a key example here, and if such aspects of our lives do become increasingly interconnected through real-time communications, then I think we have an even more convenient and comfortable future ahead of us. At the same time, this will also make our communications infrastructure ever more important.

To deal with these changes, we will no doubt need new mechanisms and forms of security that involve not only government and communications carriers but also the companies and individuals that use communications services. We do not yet have the right answer to all of this, but what is certain is that we will need to remain consistent in our efforts to deal with the ongoing arrival of new threats.

DDoS Attacks

Hiroshi Tamaru
Security Business Development, Advanced Security Division

The term "DDoS attack" began popping up in Internet-related news around 2000, and IIJ has observed many DDoS attacks over the years. Here, I would like to look back at the past 20 years or so as it relates to this and then explore what the future may hold.

We launched our first DDoS protection service in 2005. The trigger for this was a DDoS attack on a customer web server that overloaded the firewall protecting it, rendering it impossible to control. The high load on the firewall was due to an abnormally high volume of requests and a massive amount of half-open TCP connections, which caused the connection management tables to overflow and forced the system to generate and process a huge volume of access logs.

The day before we experienced this DDoS attack, we did have some warning signs, including a large number of port scans being performed, and so we were on alert and had taken precautions. In the end, however, we were unable to fully protect the customer's network from the DDoS attack. This experience prompted us to think hard about what countermeasures we might be able to implement on IIJ's equipment, and I still remember us talking and talking about it—at our desks, during meals, in the break room, everywhere.

Background to DDoS attacks

Attacks like these come with background context, and there have been changes over time in this regard. A past attack with historical underpinnings was one that originated in China and was associated with the date of the Manchurian Incident. We observed this pretty much every year from around 2005, but this activity seems to have subsided over the past 10 years. Given the propensity for attacks to occur on historically significant dates like this, IIJ continues to be alert to such attacks. Meanwhile, DDoS attacks carried out by Anonymous as a form of protest are on the rise. Japan has seen such DDoS attacks carried out in opposition to whaling and dolphin fishing, to protest against the discharge of treated water from the Fukushima nuclear power plant into the ocean, and to express opposition to Japan's position on the situation in the Middle East.

When the background involves history, politics, animal welfare activities, or environmental or human rights advocacy, the attacks are often organized ones. Recently, however, we have started to see attacks on service providers in the gaming and entertainment industries for what are apparently personal reasons. You may have heard the phrase DDoS as a Service. The fact that anyone can now easily and cheaply purchase a service that will perform a DDoS attack is a key factor behind this recent trend. Something as trivial as a personal grievance in an online game or an employee's offhanded posts on social media or a message board can trigger an attack on a company.

■ DDoS attack and defense

DDoS attacks, as is well known, can be broadly categorized into resource consumption attacks and volumetric attacks. From a defense perspective, another way to think about it is whether the attack is one in which the source addresses can be spoofed or not.

In attacks like TCP Connection Flood, HTTP Slow, and HTTP Request Flood, for example, a TCP connection must be established, making it relatively difficult to spoof source addresses. With these types of attacks, you can expect to mitigate the impact to an extent by tightening connection criteria when the attack is taking place. Effective steps may, for example, include shortening the timeout for idle TCP connections, putting priority on allowing connections from specific regions, and restricting access based on country/regional IP address allocations.

TCP SYN Flood, on the other hand, is an example of an attack in which source addresses can be spoofed. It has been around for quite some time. With TCP connections, methods based on the TCP protocol can be used to determine whether the sender actually exists or not. Depending on the confirmation method implemented in the DDoS mitigation device, however, the sender may need to retransmit packets (a browser reload in the case of HTTP/HTTPS), or the firewall may deem confirmation packets sent by the DDoS mitigation device as invalid and discard them, thus making an incorrect determination, and so the impact of these factors needs to be taken into account.

Reflection attacks, which exploit responses sent by devices connected to the network, use many protocols not normally used on the Internet, like Memcached, SSDP, MSSQL, ARD, and SNMP. These attacks can easily be mitigated by setting up filters. In the case of DNS and NTP, the ability to restrict source addresses, if this is possible, can make it easier to guard against attacks. The steps we are taking as an ISP to prevent source-address-spoofing attacks include implementing SAV (Source Address Validation) methods such as uRPF.

■ Choosing DDoS countermeasures

Methods of protecting services and infrastructure from DDoS attacks include building a dedicated on-premises DDoS mitigation appliance and using services offered by CDN providers, cloud services, or ISPs such as IIJ.

Attacks that exceed 100Gbps are not uncommon these days, and this can easily exhaust available bandwidth with on-premises solutions, so you may need to consider using another service entirely or in combination with your on-premises solution.

The services offered by CDN providers tend to use anycast and the like to make it possible to disperse attacks by having a broad network of receiving nodes across the globe. They also commonly provide streaming and WAF services in combination with this, making these services well suited to Web systems.

The services provided by ISPs like IIJ, on the other hand, make it possible to protect not only publicly exposed systems but also office Internet connections used for business purposes. If your ISP does not provide DDoS mitigation services, you can protect your network using a cloud-based service, but it must be noted that such services may come with certain restrictions to facilitate route control.

■ Outlook

Increasing PC and server performance means that services with 1Gbps or 10Gbps bandwidths are now available to ordinary household customers. A whole range of services is available via the Internet now that all sorts of devices like surveillance cameras and home appliances have online capabilities. But we also continue to see cases of the OSes and firmware on home routers, surveillance cameras, NAS devices, and the like being infected by malware that turns them into bots for use as DDoS attack sources. In the hopes of mitigating the damage caused by DDoS attacks, we at IIJ will continue to highlight the importance of properly updating software not only on PCs but also on these sorts

of devices, and the importance of installing software updates and addressing vulnerabilities on public servers.

We will continue to look at how we can upgrade and configure our environment to detect and block attack traffic in both directions so that we can not only protect our customers from incoming attacks but also ensure they are not implicated in outgoing DDoS attacks, our ongoing aim being to build a safe and secure Internet that people can use with peace of mind.

The Greatest of Frustrations

Mamoru Saito
Director, Advanced Security Division

We respond to cyberattacks directed at our customers on a daily basis, and in many cases we treat the associated problems experienced by our customers as if they were, in a sense, natural disasters. As a private-sector security provider, we are not in a position to attempt to catch the perpetrators even if a cybercrime has been committed. We focus on investigating the technical causes, minimizing the impact, and working to restore systems. We do not seek to identify the perpetrators or confirm their location in the way a judicial entity would. Instead, we simply track down and trace information relevant to our being prepared for the perpetrators' next action.

Even so, as someone who has worked in security for many years, there was just one case in which I really felt the desire to catch and punish the perpetrator. This was the case of Antinny, which caused a whole slew of serious information breaches.

Antinny is malware that runs on Windows PCs on which the P2P file-sharing program Winny is installed and has the ability to send files on the PC to external parties without the PC user's consent. Leaving aside the pros and cons of Winny as a system[*1], the advent of Antinny made installing and using Winny an extremely risky proposition.

Antinny tricks users into running it by adopting a deceptive file name that makes users think it is a video file or the like. Its actual malicious behavior is to search for images and office files on the PC and copy them to Winny's upload folder, causing them to be shared externally. This resulted in many information breaches, including the leaking of people's personal photos, and the leaking of work-related files that people had brought home from the office, which then escalated into corporate data breaches and the like. Once a month, it would also bundle screenshots and files stored on the PC into a compressed archive and upload it to the copyright infringement query section of the Association of Copyright for Computer Software's website. These uploads drove DDoS attack-levels of traffic to the association's web server, at times making the website inaccessible.

None of Antinny's functions take advantage of vulnerabilities or privileges. They simply perform actions that a user with normal privileges is permitted to perform, such as copying files to Winny's file-sharing folder. Because Antinny compromises Winny users and sends their information to a copyright management organization, it is conceivable that Antinny's creator intended it as a type of joke or prank program designed to send somewhat of a message. Its proliferation, however, had profound social implications. It disrupted people's lives and impacted on the activities of many businesses and other organizations.

Efforts to combat Antinny also lagged across the board such that the malware was able to rage on for many years. In 2004, the ISP security organization Telecom-ISAC Japan (currently ICT-ISAC Japan), working with the Association of Copyright for Computer Software, made a successful attempt to control the DDoS attack-levels of traffic generated, but it also showed that exercising that control on an ongoing basis would be highly costly. On the antivirus front, perhaps because Antinny was seen as a uniquely Japanese phenomenon or perhaps because of Winny's unique environment, it was several years before many of the antivirus products on the market gained the

*1 Winny was not equipped with communications optimization features, so it would constantly send data over long distances across the network, putting unnecessary strain on network capacity and causing poor communications quality due to congestion between many ISPs. So it was an application that had considerable side effects from a communications business perspective as well.

ability to remove Antinny[*2]. Eventually, owing to revisions to Japan's Copyright Act, the number of Winny users declined dramatically, and the impact of Antinny also diminished as the issue faded away.

So it is that Antinny is no longer something we need to worry about, but its creator remains at large, and it is extremely frustrating to think that he or she may still be living a normal life in Japan to this day. I think we need to have a proper discussion about whether Antinny constitutes a virus and whether we can consider its effects to be criminal. At this point, with so much time having passed since it was brought under control, it would be a tough ask to dig back into the Antinny issue and discover the real culprit. That said, when the next Antinny rears its head, it is my hope that we in Japan will be able to mount an appropriate response.

The Impact of Snowden

Masafumi Negishi
Head of the Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division

It is impossible not to mention Edward Snowden's revelation of US state secrets when discussing events that impacted heavily on our society during the 2010s and 2020s. In June 2013, Snowden, then working for the US National Security Agency (NSA), appropriated a huge number of classified documents, which included top secret information, and disclosed them through multiple media outlets. A particularly shocking revelation from the information leaked was that of the comprehensive surveillance of the Internet and telephone lines, predominantly carried out by the Five Eyes intelligence alliance, which includes the United States. In the wake of the September 11 terrorist attacks of 2001, the US enacted legislation to strengthen wiretapping and the interception of communications for the purpose of monitoring terrorist activity. This resulted in an immensely vast and comprehensive surveillance network being established and operated, with implications not only for hostile actors but for US citizens and other countries as well. It was also revealed that major US telecommunications carriers and major tech companies, including Microsoft, Google, and Apple, were cooperating in the building of surveillance systems and collection of information in accord with law enforcement agency requests and court orders.

These leaks sparked criticism not only in the US but around the world as people raised concerns about privacy and other human rights violations due to excessive surveillance, and efforts were subsequently made to counter these surveillance networks. The practice of encrypting communication routes became widespread, led in particular by the aforementioned tech companies, and we saw a rapid rise in the encryption of inter-datacenter communications, the use of encryption by default on service-providing sites, and so forth. As a result, encrypted HTTPS communications as a proportion of all traffic from browsers rose to 70% in 2018 and to over 80% in 2020[*3]. IIJ's observations for 2023 also show that over 70% of broadband communications are encrypted[*4].

The TLS 1.3 standardization work that began in 2014 also incorporated encryption methods requiring handshake encryption and forward secrecy to protect against network monitoring. The standardization of the DNS over TLS (DoT) and DNS over HTTPS (DoH) protocols for encrypting DNS communications has also moved ahead, and these protocols are now in the process of widespread uptake. Hence, Snowden's revelations have had a major impact on the formulation and widespread adoption of technical standards.

This has an impact not only on communications but also on devices like smartphones. Major messaging services like Apple, WhatsApp, and LINE, for instance, support end-to-end encryption (E2EE), a strong encryption system that prevents anyone on the communications route, and

*2 Initially, only a handful of vendors like Trend Micro were able to get rid of Antinny. After Microsoft addressed the issue and revealed that it had removed Antinny from many systems, a lot of other antivirus vendors followed suit. For its service in this case, Microsoft received a Minister's Commendation from Japan's Ministry of Internal Affairs and Communications and a letter of appreciation from the Association of Copyright for Computer Software.

*3 Based on Firefox telemetry data (https://letsencrypt.org/stats/).

*4 See "1. Periodic Observation Report" in IIR Vol. 61 (https://www.iij.ad.jp/en/dev/iir/061.html).

even the service provider, from reading the contents of your messages. Apple, Google, and others have been enhancing their smartphone encryption features since 2014, using encryption to protect user data stored on such devices and cloud services. While these efforts protect the security and privacy of users, they also benefit criminals. Since the late 2010s, there have frequently been reports of these mechanisms hindering criminal investigations by making it impossible for law enforcement agencies to extract data from devices seized from suspects. In an attempt to improve this situation, government agencies in the US and Europe are moving to regulate the cryptographic features that the technology industry provides.

Snowden's revelations also illuminated cyberattack activity against other countries by intelligence agencies in the US and elsewhere. The NSA, in particular, has some of the world's most advanced cyberattack capabilities. It engages in a range of espionage, including vulnerability research, the development of attack code and malware, and the use of this to infiltrate organizations in other countries. The large-scale WannaCry outbreak of May 2017 is an example of how the NSA's activities directly affect us. To infect Windows machines, WannaCry used attack code and a backdoor program that had been leaked by a group called The Shadow Brokers. The Shadow Brokers had stolen the leaked data from an attack group called the Equation Group, and it was later revealed that the Equation Group was actually an NSA cyberwarfare unit. While the truth remains unclear, the Shadow Brokers are suspected of having ties to Russia, and the US has issued an official statement claiming that the WannaCry attack was the work of North Korea. And so it is that the Internet, an essential part of the infrastructure of our daily lives, is also a theater not just for cybercriminal activity but also for constant battles among multiple attack groups with connections to nation states. The multiple layers of such activity all have an impact and make for a complex Internet environment, and this presents a huge challenge for us that we must solve if we are to provide safe, secure networks that everyone can use with peace of mind.

The Changing Face of Security Operations Centers

Tsutomu Nakajima
Manager, Data Analytics Section, Security Operations, Advanced Security Division

From black to white

Security operations centers (SOCs) started rising to prominence in Japan as security monitoring groups or facilities around 2000. Initially, they were housed in dim, windowless rooms lined with displays, and only security analysts—engineers with a deep knowledge of network security—were given access to the monitoring systems. This picture began to change around 2015, with SOC equipment being reimagined to adopt bright colors, and IIJ's SOC, which we renovated in 2017, also turned into a more welcoming, comfortable space for engineers (Figure 1, Figure 2).

In conjunction with this, to ensure we could respond to increasingly sophisticated threats, we also reimagined the way our SOC and its operations are organized. In the past, the SOC essentially referred to real-time security monitoring, but we now have many security engineers stationed within

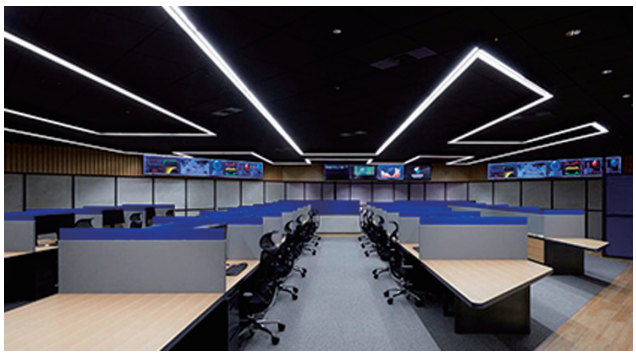

Figure 1: Operations Room

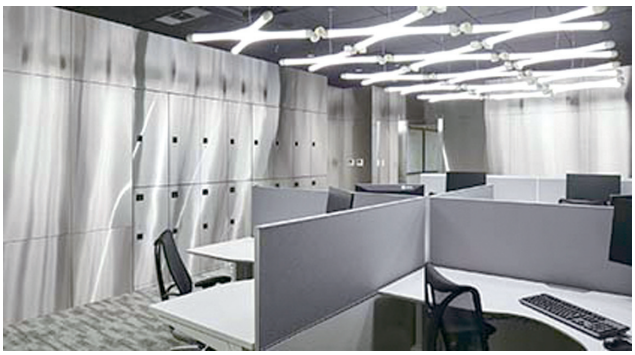

Figure 2: Security Lab

or close to the SOC to ensure that the right people are able to come together and collaborate on incident responses when needed. With diversity also becoming an increasingly important social theme, IIJ's SOC has also adopted a value system that welcomes a diverse range of engineers to the team, united under the single purpose of dealing with security incidents.

From networks to devices

The SOC monitors a variety of devices. In the past, firewalls, IPSs, and the like in the form of security appliance boxes located at network boundaries to monitor traffic along communications routes were the mainstream. A lot of the significant security incidents in the 2000s were attacks on servers, and so the SOC's main role was to protect servers necessary for ensuring business continuity.

As a security analyst, I sensed change in the air when email-driven attacks, particularly targeted attacks, began rising to prominence, and it was around this time that I realized, intuitively, that monitoring server segments alone would be insufficient to safeguard the systems we sought to protect. In recent years, the SOC has also had occasion to monitor wide-ranging attacks from indiscriminate malware such as Emotet as well as internal misconduct at some organizations. Attacks on public servers remain, as always, a feature of the landscape, but with attack targets having been expanded to include client devices, we now also need to monitor internal-to-external and internal-to-internal communications. Firewalls are one of the main monitoring tools, and the evolution of firewalls to incorporate multi-featured unified threat management (UTM) technology, and then next-generation firewall (NGFW) technology facilitating application-layer analysis, has improved communications traffic visibility.

Meanwhile, with communications routes and communications themselves increasingly being encrypted, more than a few SOCs now monitor not just the network but also device processes and logs via technologies like endpoint detection and response (EDR). Alongside attacks exploiting vulnerabilities, cases of personal credentials (used in authentication) stolen through whatever means being used in initial attacks are also on the rise of late, and so the management of such credentials has also become an issue.

The role of SOC engineers

The role of the SOC is not to maintain normal operating conditions but to discover abnormalities. Even if a monitoring system does not raise a security alert, any signs of suspicious activity still require investigation. Back when the SOC focused primarily on network monitoring, our skilled security analysts, guided by their knowledge and experience, would uncover security incidents by looking through seemingly ordinary event logs to spot anything that just didn't look right. But as such logs grow in variety, there arise limits to what can be achieved through manual monitoring of the complex, intertwined data generated. And in addition to monitoring data in real time, we also now need to recursively investigate past data, and time considerations here also make manual investigations difficult.

These days, the knowhow to detect anomalies comes built in as security sensor detection rules and security information and event management (SIEM) rules, and this has reduced the associated engineer workload and served to make such technology more common. AI is used to perform data-based analysis to reveal anomalies that humans would otherwise not notice, and to mitigate the limits of human memory. Yet attackers can similarly benefit from AI and thus continue to discover new security holes.

People have always been at the heart of the SOC, and even with all of the automation and systemization available today, the knowledge and experience of engineers continues to have a major influence on the SOC's analytical capabilities. "Updating" ourselves as SOC engineers every day can help us to respond to new attacks as well.

3.2 Conclusion

This article has presented the personal reflections on the past 30 years of a number of our security professionals. The Internet's evolution has by no means reached an end. In just the past few years it has redefined our daily lives through the development of telework environments, the proliferation of AI, and the like. The Internet landscape will no doubt continue to change ahead, with new incidents and challenges arising along the way. To protect our modern way of life and keep everyone safe, we will continue to stay ahead of these changes and strive to address the new challenges that arise.