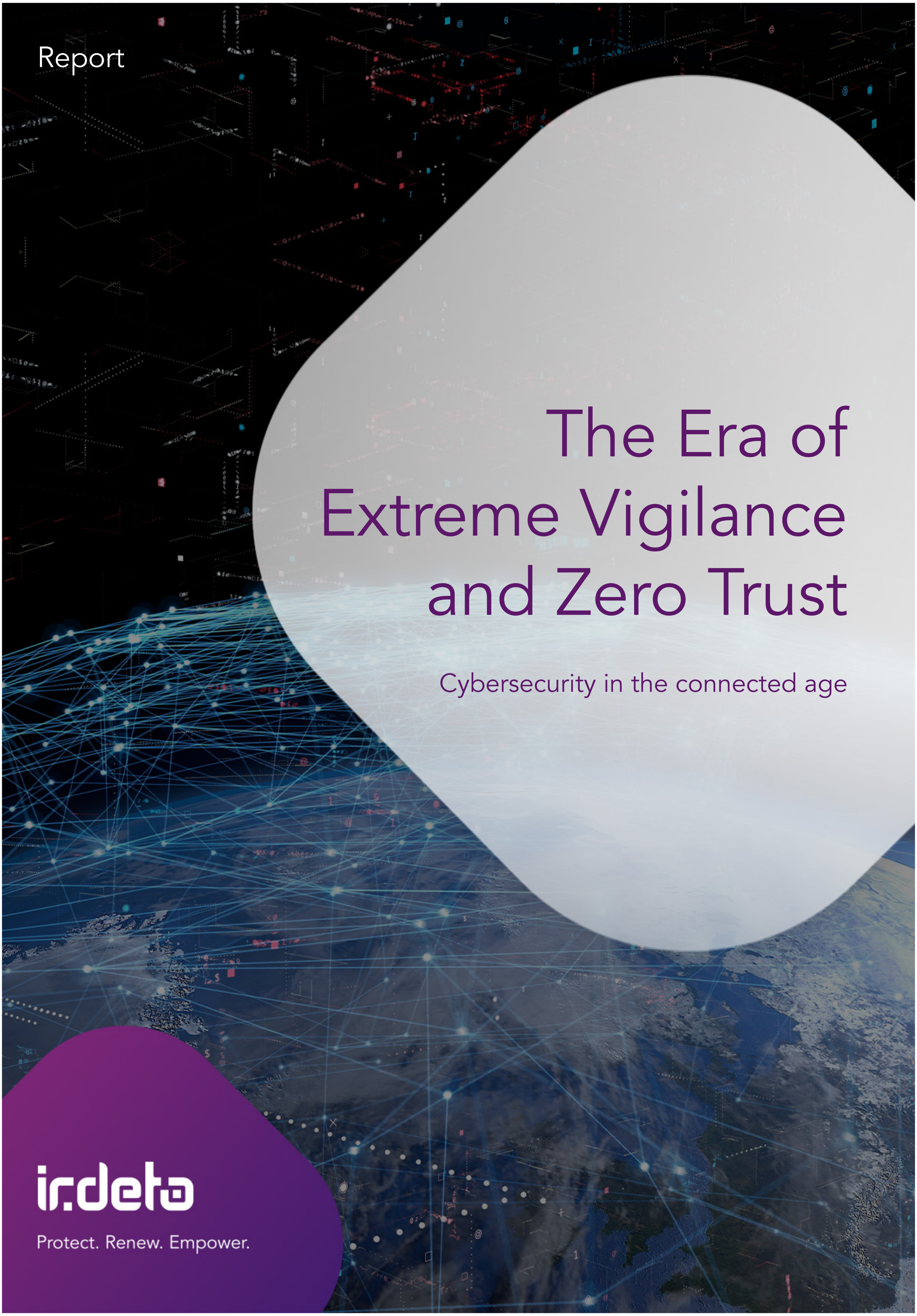
Report



The Era of Extreme Vigilance and Zero Trust

Cybersecurity in the connected age

irdeto

Protect. Renew. Empower.

It is both a blessing and a curse to live in the connected world. The very things that make it one of the most exciting eras in our history, also make it the least secure. Because behind every development, every technological advancement and every connected device, lurks a pirate or hacker, ready to capitalize on vulnerabilities and profit off of weaknesses.

Preparing for the peak

Although 2021 was the most prolific year for cyberattacks and piracy, Irdeto experts predict that we're far from seeing the peak of activity. Cyberattacks and piracy are becoming increasingly sophisticated, and recruitment of new pirates and hackers is at an all-time high, partly driven by the Covid pandemic. But another key driver is consumer demand: from video entertainment and video games to connected cars with the latest amenities, customers demand the best that technology can offer. But companies that rush to deliver on that demand can become the architects of their own demise.

Like many companies, Irdeto applies a Zero Trust Architecture approach to keep its own systems safe. That includes continuous employee training, multi-factor authentication to access the company network and any sensitive data, and automated defense systems that alert us whenever any unusual activity occurs. After all, breaches can happen anywhere, at any time, with even the slightest human error.

There's a silver lining

It wasn't all bad news in 2021, and there is reason to be hopeful in 2022. An increase in legislation and regulation around cybersecurity has made identifying, catching and prosecuting cybercriminals more effective. And developers are finally being held to stricter standards when it comes to new connected devices and services. In corporations around the world, cybersecurity is finally becoming a must-have, instead of a nice-to-have. And all of these together help strengthen our defenses.

Irdeto's innovations are not just hardware and software, but also the data, insights, and intelligence that more than 50 years in the busines brings. And, as we move forward into 2022 and beyond, Zero Trust and constant vigilance will continue to be the order of the day. At Irdeto, we aim to continue to secure our customers' freedom to do business without disruption. Safeguard their assets and their reputations. And fight the plague of cybercriminals by any means necessary.

Saluting Our Colleagues Around the World

Irdeto would be nothing without the people who are part of our team. Every day, they offer their talent and commitment to making the cyberworld a safer place. And we are grateful for the contribution that each employee makes.

Like every other company in the world, Irdeto had to adjust to life during a pandemic. But few could have predicted how seamlessly our colleagues would adjust to the change. Seemingly overnight, our teams smoothly transitioned from working in our offices around the world to working from home, with little impact to customer delivery or service.

It was helpful that Irdeto was one step ahead. We had already been working on a hybrid working model for the company, based on feedback from our employees. Covid simply accelerated our efforts, and resulted in the Work Hard Anywhere framework, now fully up and running.

A global company like ours has had a unique perspective on this pandemic, because we are able to see how it directly impacts each country. The differences were sometimes significant. We were there for our people when times got really tough. Sometimes, even assisting in getting medical supplies to colleagues and family members who desperately needed them.

Our hearts and thoughts are with our colleagues around the world who lost loved ones or became ill themselves during these challenging two years. We will continue to do everything we can to show you that being part of Irdeto means being part of a family. We will continue to look out for our people with the same diligence and care with which they look out for our customers. Because we couldn't be us without our people.

Chapter 1

Taking Control of the Pirate Plague

Piracy is nothing new. As long as companies have been making content, pirates have crafted new ways to steal it. And every time one hole in the system gets plugged up, the plague of pirates finds – and gnaws through – another vulnerability.

What makes the current era unique is the level of sophistication and commoditization that have become the hallmarks of cybercriminals. The cybercrime business model offers free-to-use, commission-based services that include tech support, so even criminals with no technological knowledge can set up scams in minutes, pay nothing out of pocket, and profit off of system vulnerabilities and human error.

In 2021, Covid-19 forced more people to stay at home than ever before. This captive audience was a breeding ground for content creation, and we saw a boom in game and video entertainment development. This combination of more content and a larger field of attack created a perfect cyber storm: and pirates took advantage whenever they could.

Catching the big phish

Phishing continues to be the crime of choice among bad actors. But they're not limiting themselves to emails. Phishing has taken place in SMS and in text apps, on social media, in games, on collaboration platforms and in online marketplaces. And the more sophisticated the phishing attempts get, the harder it is for companies and consumers to recognize them as phishing.

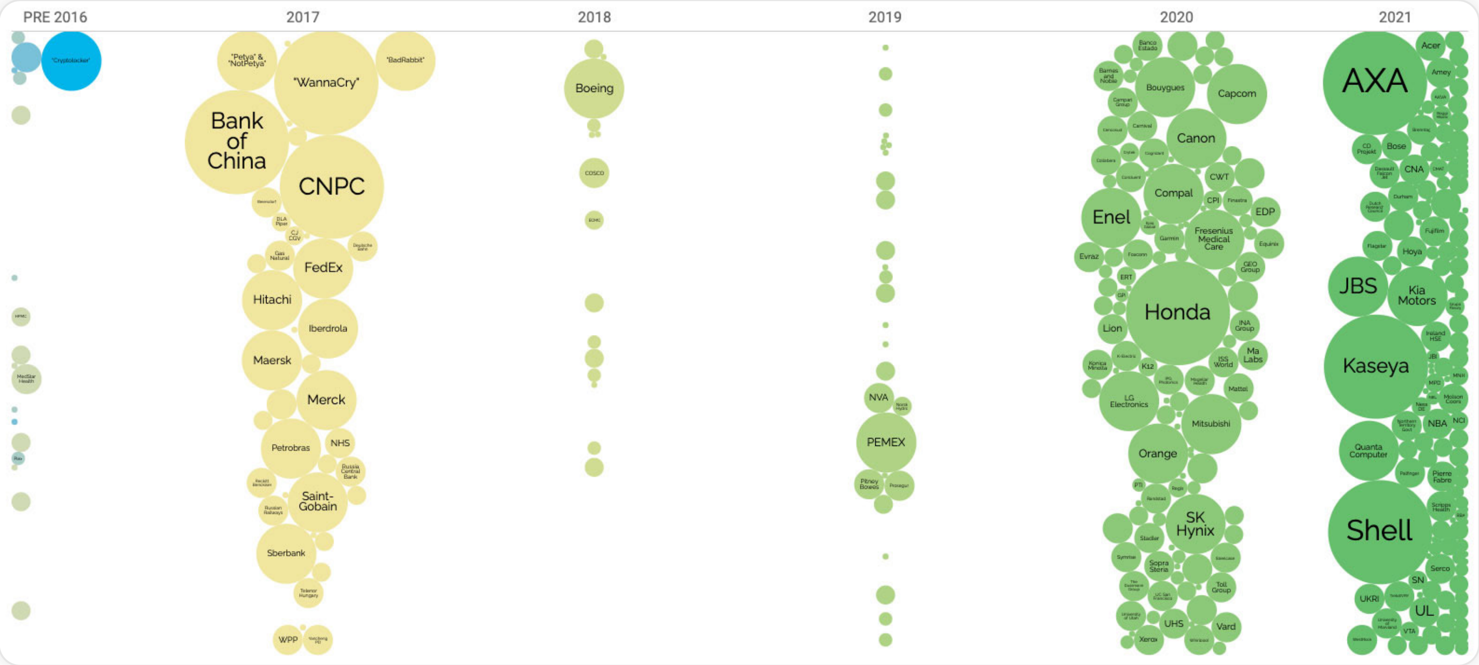


Figure 1.
Ransomware Attacks by year

Source:
informationisbeautiful.net

Keeping constant watch

Since the phishing threat is likely only to grow and gain sophistication in the coming years, nothing less than 24/7 hyper-vigilance and regular staff training can protect a company from these attacks. With as little as 45 seconds of recorded audio and video from a published interview with a C-Suite executive, phishers can develop a Deep Fake that appears 100% legitimate. Like a video image that looks like your company's CEO, asking you to transfer funds to a specific bank account. However, the content is entirely fabricated. But it only takes one employee who falls for the fake to give the hacker access to a company's systems.

That's why, in addition to automated and constant protection in the form of software threat intelligence and defense solutions, a Zero Trust security culture will be essential for businesses in the future. Irdeto works to help companies understand the nature and magnitude of cyberattacks, and encourages customers to regularly and consistently raise awareness within the organization about potential threats. As the hackers develop and improve their methods, so too must companies improve their campaigns against them.

Aiming solutions at the biggest targets

The two industries most vulnerable to attacks – and most attractive for attackers – continue to be video entertainment and video games. High consumer demand for new content, rapid development of that content, and often out-of-date consoles and electronics are simply too tempting for bad actors. They constantly uncover vulnerabilities in distribution systems and exploit them for profit.

Video entertainment in particular is a challenge. With the explosion in streaming services and connected content, the entire production process – from filming to production to distribution to consumption – offers opportunities for hacking. Here, too, we are seeing growing sophistication in attacks. Pirates exploit vulnerabilities in Over-the-Top (OTT) media services and Content Distribution Networks (CDNs), often piggybacking off of the operator's system and redistributing content. In this way, they can capture content from the OTT and CDN servers, and pay no cost to access and redistribute pirated content.

Only robust security intelligence and defense solutions can help OTTs and CDNs track piracy back to its source and switch off the hacker's access. Then, it is up to the company to determine the level of response, from simply plugging the hole that allowed the hack, to tracking down the offenders and prosecuting them.

For video games, security solutions must keep pace with the hackers and cheaters they are guarding against. For both the 'good guys' and the 'bad guys', action begins the moment a game is released. And that means that protection services must be as robust and up-to-date as possible, and must constantly be improved upon to stay one step ahead of the bad actors. That means infiltrating hacker groups, collecting intelligence, learning and improving techniques at every turn. Irdeto works to monitor and evaluate potential threats for game publishers, and prioritizes the threats that pose the biggest risk. At the same time, we monitor older games and systems and keep them constantly and continuously updated. After all, long after the game has lost its newness, it remains an attractive target.

Playing the long game

When it comes to anti-piracy, there is no silver bullet. No one, sure-fire way to keep systems safe. As threats continue to grow and mature, we must play the long game of security. That means that security professionals must be the eyes and ears of an organization, make systems as resilient and ready as possible at any given moment, and constantly re-evaluate protection software and methodologies to ensure they remain robust. We must remain quick and nimble, adjusting to each new development and growing our strength and resilience alongside the growing threat.

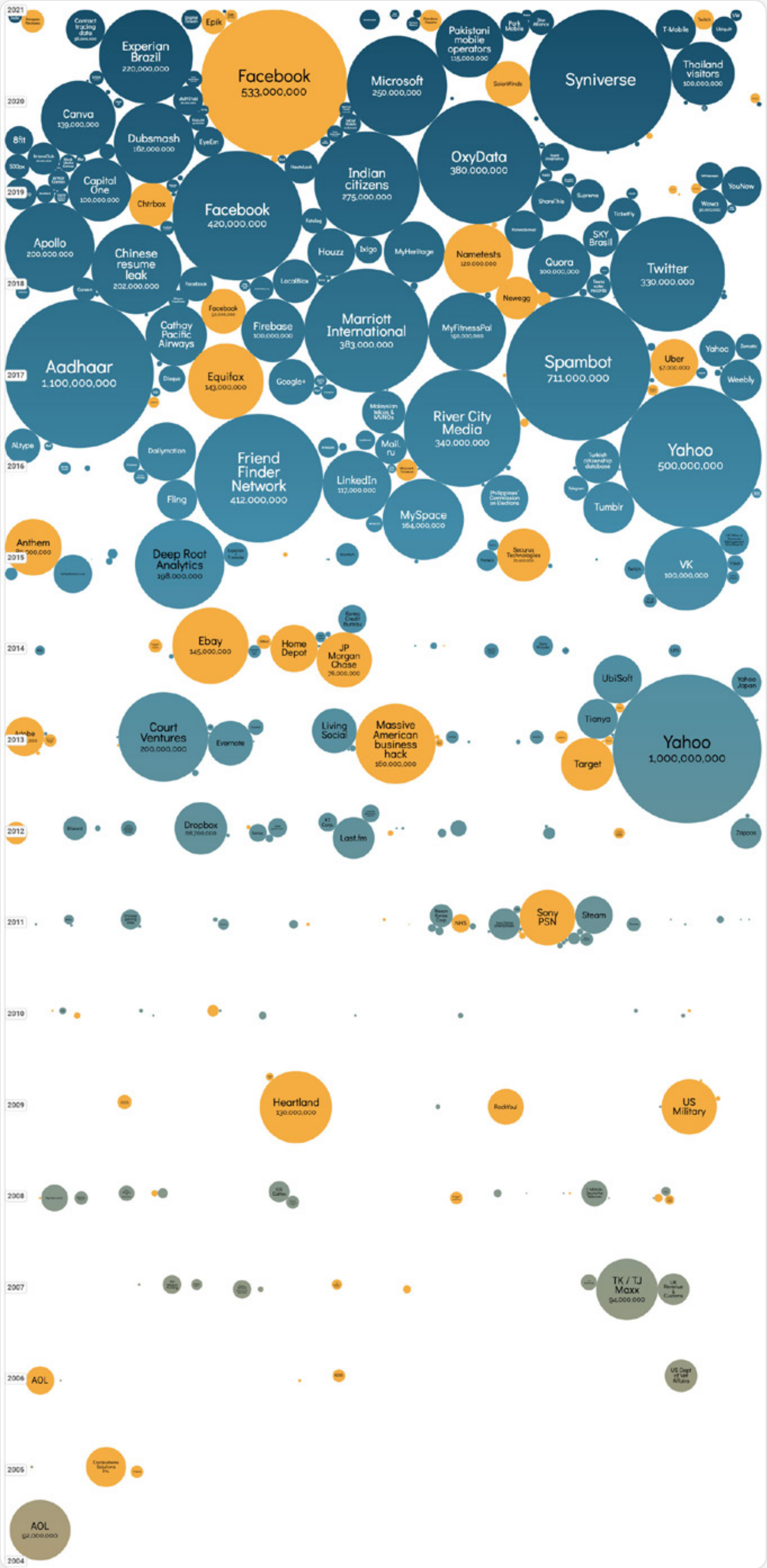


Figure 2.
Data Breaches & Hacks by year

Source:
informationisbeautiful.net

Chapter 2

Welcoming the Long Arm of the Law

Perhaps one of the most exciting and welcome developments in the past few years has been the increase in regulation and legislation. For the first time, governments are taking broad-scale action to stop the relentless flow of piracy and cybercrime. And while there's still a long way to go, and many complicated challenges to overcome, regional and international law enforcement agencies are beginning to make significant progress.

Joining forces for change

Given the complexity of the cybercrime issue, no single organization – public or private – can combat the problem alone. Especially considering that cybercriminals can literally operate from anywhere in the world, and their networks of bad actors have been able to grow and multiply virtually unchecked for years. Often, it is challenging to determine legal jurisdiction and identify key criminals within the confines of legal and investigative processes. It can often take years to build an effective case against a cybercriminal, in which time the offender can cease activity or move location.

Now, we see that law enforcement is working together across many countries and capacities, bundling their efforts and achieving real results. Organizations like the Audiovisual Anti-Piracy Alliance have been working with governments, law enforcement and private industry to advise on appropriate legislation, effective investigation and raid techniques to ensure that the relevant evidence can be seized to build a strong case against offenders. Because of these coordinated efforts, we've seen some of Cybercrime's Most Wanted finally get indicted for their offences.

Bringing down Omi

Most recently, Bill Omar Carrasquillo, known in the cyber underworld as 'Omi in a Hellcat', and two of his associates were indicted for crimes related to their piracy of content from several major video entertainment content providers. The co-conspirators' income from their alleged activities is estimated to be at least US$34 million. Nearly US$40 million in assets – including luxury cars, jewelry, and real estate – was seized in the raid on Carrasquillo's home. If convicted, Carrasquillo faces up to 514 years in prison, and his two associates 244 and 130 years, respectively. Although the three deny any wrongdoing, the FBI has collected substantial evidence to support the indictment.

Voksi retires and REvil falls

The Bulgarian hacker known as 'Voksi' systematically worked to circumvent Denuvo by Irdeto's anti-tamper and anti-cheat software for video games. After collecting evidence against him, Denuvo filed a criminal complaint in 2018, leading to the Bulgarian Police's raid on Voksi's home. Soon after, his hacking forum REVOLT went offline, and Voksi announced that he'd be retiring from the game-cracking business.

As recently as January 2022, 14 members of the REvil ransomware gang were arrested in Russia. Although the arrests are viewed as a political power play, it is still a big win to take down the suspected Colonial Pipeline hackers.

Unfortunately, for every cybercriminal that gets caught, dozens more stand ready to take their place. But catching some of the most highly visible and popular actors in the hacker world will perhaps deter some from going down the same path. At the very least, the intelligence and information law enforcement acquires from these arrests only bolsters their capabilities and makes the next arrest that much easier.

Assembling the global posse

Around the world, governments and law enforcement are giving their attention to – and increasing their legislation against – the growing threat of cybercrime. In 2020, the European Commission proposed the Digital Services Act package: legislative initiatives aimed at protecting digital content users' rights and establishing a level competitive playing field for content producers.

In the past year, American President Joe Biden has announced several programs to combat cybercrime. These include an Executive Order on Improving the Nation's Cybersecurity, which places strict new standards on the cybersecurity of all new software sold to the U.S. government and strongly urges private companies to ramp up their security efforts. The Executive Order also addresses phishing and other types of cyberattacks, and the additional attention the American government will be paying to these initiatives. The U.S. government's launch of the Stop Ransomware site offers services and information to help address the ransomware plague.

INTERPOL led one of the most extensive and interesting cases of cross-border collaboration to take down cybercriminals in 2021. In a four-year operation that spanned five continents, 17 countries, 19 law enforcement agencies and several private companies, Project Quicksand resulted in at least seven arrests, including two Romanian hackers believed to be responsible for 5,000 infections and half a million US dollars in collected ransom. Private companies working within Quicksand developed tailor-made decryption tools that unlocked ransomware attacks, which is estimated to have saved around US$475 million in potential losses. Looking forward, INTERPOL's US$3.1 million INTERPOL Stop Online Piracy (I-SOP) initiative will continue to ramp up efforts to slow the growing wave of piracy.

Learning, growing and moving forward

These coordinated efforts to take down cybercriminals are just the tip of the iceberg. Considering that millions – or even hundreds of millions – of dollars and euros in illegal profits can be made from a single case, the impact of cybercrime begins to take shape. The discussion around a minimum global standard for cybersecurity, and whether there's a need for it, is ongoing.

What is more evident than ever is addressing the problem from multiple angles will continue to be necessary. Law enforcement and governments will learn from every investigation, every raid and every arrest. Legislation will become more visible and harder to avoid. In the meantime, threat intelligence and defense systems will continue to improve, based on collected evidence. And, as the long arm of the law continues to reach deeper into the dark world of cybercrime, we will begin to uncover the keys to bringing law and order to this Wild West landscape.

Catching Another Type of Criminal

Whenever possible, Irdeto aims to make a contribution to our world and our society by doing what we do best. For the fourth year in a row, Irdeto is working with the African Wildlife Foundation (AWF) to help stop poaching and illegal online animal trade. With a combination of our cybersecurity products and AWF's commitment to helping wildlife thrive in Africa, we are hunting down illegal actors and helping to prosecute them. A win for AWF, and a win for Irdeto. An overwhelming number of Irdeto's colleagues support this initiative.

Chapter 3

Facing the Facts about Video Entertainment Pirates

The days when video entertainment piracy was seen as a nuisance or an isolated problem are long gone. Lone wolf pirates and individual breaches have been replaced by extensive international networks of pirates, working efficiently and effectively to steal desirable content. Today, video piracy is a multi-billion-dollar industry, complete with the infrastructure and business models to support extensive growth and long-term survival. Operators that want to protect their valuable content need to take a fresh look at this age-old challenge, and adapt their thinking to keep up with the rapid pace of piracy development and consumer behavior.

When a pandemic fuels a plague

Video piracy was an issue long before Covid took hold. But when the pandemic hit, it fueled the piracy plague in some significant ways. Distributors started releasing premium content more quickly, since theater releases were not really an option anymore. What's more, as some people faced financial difficulties because of the pandemic, they looked to save money wherever they could. And if they can get all the premium content they want for extremely low rates, then the idea of consuming pirated content is suddenly much more attractive. Just as in any other market, increased supply met increased demand, and 2021 saw exponential growth in video piracy.

In addition, the sophisticated piracy industry – illegal though it may be – became too hard to resist for those who needed new sources of income. The advanced and easy-to-use systems that drive piracy today provide a low threshold for entry of new pirate recruits. They don't need to know anything about the technology to get involved. For a few hundred euros, they can set up their own piracy organization, complete with customer support and troubleshooting, and quickly start earning cash.

Higher quality for discerning customers

Remember the days when pirated content came from someone sitting in a movie theater with a video camera, recording the film as it played? The proliferation of pirated content was somewhat limited by the low quality of the content. But that's all changed. Pirates now are tapping directly into the digital feeds and stealing the same, high-definition versions of films and programs that distributors are sending out. This not only makes the pirate's product much more desirable, but also makes it harder for consumers to differentiate between pirated and non-pirated content. The whole system feels 'normal' and acceptable, more than it ever did before.

Take a look around

Distributors and operators that want to get ahead of the piracy need to look deeply into the issues that cause it. How do the leaks happen? Why do they happen, and who is behind them? But instead of simply plugging up the holes and walking away, today's anti-piracy activities must be continuous, 24/7 endeavors. After all, the piracy is, too.

Irdeto applies an adaptive and continuous protection infrastructure that is also real-time. After all, it does no good at all to catch a pirate two hours after he's illegally distributed a football match through pirated channels. We need to catch him in the act, and shut down his channel when it matters most.

Watermarking and beyond

Watermarking is a highly effective way to protect against piracy. It enables operators to track where and how their content is being distributed, and catch the pirates red-handed when they distribute on illegal channels. But watermarking is just the beginning. The sophistication of modern piracy requires sophisticated tooling to combat it. Tools like Irdeto's RDK Hybrid Stack and Certified Secure Experience offer new levels of middleware protection that enables operators to ensure secure access for legitimate app vendors, while keeping the lurking pirates at bay. It also makes the app onboarding process easier.

Of course, increased regulation and legislation can help, too. Before effective legislation was in place, operators had to pursue pirates on their own, and foot the bill if they chose to take a pirate to court. New legislation can make piracy a criminal matter instead of a civil one, and relieve the burden of litigation from operators' shoulders.

Beating pirates at their own game

Distributors can fight back and beat pirates at their own game. Consolidation of independent operators and the creation of super aggregators can make the distribution network stronger and help vendors that are struggling to stay afloat in these challenging times. There's strength in numbers for operators, just like there is for pirates.

Another key to managing the piracy threat is a mindset change. Not in the minds of the pirates, but in the minds of content producers and distributors. The new generation of consumers demand highly personalized content, tailored to their needs and easy to use. The rise of super aggregators will open the door to personalized viewing experiences, targeted advertising and other means to capture and retain customer bases and secure income in the changing entertainment landscape. If operators can learn from new viewer behaviors, adapt their strategies to accommodate those, and change their business models to capitalize on the new strategy, then they can secure their future in the video entertainment industry.

The piracy plague is far from reaching its peak. Only constant vigilance and adaptability will protect against it. In 2022 and beyond, Irdeto will continue to help operators stay one step ahead of the plague and adapt to the changing landscape of consumer – and pirating – behavior.

Chapter 4

Beating the Cheaters at Their Own Game

irdeto

In gaming protection services, one thing remains the same: hackers and cheats don't sleep. They don't take breaks, and they don't give up. Protecting publishers' profits and players' pleasure is a 24/7, 365-days-a-year endeavor. In 2021, gaming protection companies continued to think – and act – like hackers. And that meant no sleep for them, either.

Game publishers continue to want stable, rock-solid, long-lasting protection for their new games, whatever the platform. Especially in the first crucial months after a new game is released, when nearly 60% of profits are made. That is why Denuvo by Irdeto continuously released new versions of their anti-tamper software in 2021. The smarter the hackers get, the smarter Denuvo becomes.

Fighting for fair play

But protecting publishers' rightfully earned revenue is only half the story. Because in addition to the hackers, there are also the cheaters. Around 70% of all game developers – large or small – consider cheating to be a concern.

Statistics also show that those who take shortcuts and use cheats to gain advantages in gaming actually ruin the gaming experience for up to 60% of gamers. And as many as 77% of gamers said they'd quit playing a game that was obviously being dominated by cheaters. Piracy may kill revenue, but cheating kills the game.

Publishers continue to seek anti-cheat software that is easy to integrate, has the best detection capabilities and the fastest detection speed. All with an optimal end-user experience. But they know that chasing down cheaters never ends: it merely evolves as cheaters find newer, more clever ways to invade the system. Looking ahead to 2022, the name of the game will continue to be constant vigilance.

Mobile makes a move

The growing popularity of mobile gaming is bringing the threats into the palm of our hands. In 2022, providing more security to mobile games will be a key growth area for security companies. But perhaps one of the biggest obstacles will be mobile gaming developers themselves. A mere 38% of mobile gaming developers even know that anti-tamper and anti-cheat tools are available for mobile games. This brings huge opportunities to increase awareness in 2022, so that the mobile gaming market can be as profit-friendly and player-pleasing as their console and PC counterparts.

Increased mobile gaming security, enhanced anti-tamper and anti-cheat solutions, and telemetry services that can easily be integrated into publishers' back office will be major focus points for Denuvo in 2022 and beyond. But user convenience and ease of use must always be top of mind: players won't play if the load times are long or the game speed is not fast enough.

Searching for the streaming solution

It started with music. Consumers that once owned physical content – CDs, albums, and cassettes – easily transitioned to streaming, once the right format was uncovered. Movies and TV were next: streaming services replaced DVDs and Blu-ray as the best way to expand one's viewing collection.

Is gaming next? It appears so, with the emergence of systems like Microsoft Game Pass. Today, Netflix is busy preparing its own streaming game service, too.

But what about security? There are key issues developers should keep in mind. Even though streaming does offer some protection that regular online gaming does not, there are still some major security holes to plug up, including GDPR and user privacy. Companies aiming to release their games onto streaming services need to make security a part of the conversation in 2022.

The future is full-service

So, what does the world's best games protection and anti-piracy company do to stay one step ahead? It evolves with the industry. And that means a long-term vision to become a one-stop shop for game publishers. Denuvo by Irdeto doesn't just want to offer the latest and greatest anti-tamper and anti-cheat technology. It wants to become the one source that publishers need, and the only one they need to call.

Chapter 5

Dropping the SBOM to Secure Connected Health

Even before the Covid-19 pandemic, healthcare was already using vast numbers of connected devices to treat and monitor patients. But the pandemic spurred a significant increase in telemedicine and remote care, and the medtech community scrambled to get devices to the market to support it. But given that medical data is estimated to be at least 50 times more valuable than credit card data, connected health has become yet another breeding ground for cyberattacks. Securing and protecting these systems has become more important than ever before.

Healthcare organizations have a multitude of reasons to protect medical devices. A single hack could impact patient care, create costly downtime in hospital settings, and cause serious data protection issues that not only lead to legal and financial consequences, but cause significant reputational damage as well.

Improving the health of medtech

A recent Irdeto survey, conducted with Censuswide and Guidepoint Global, showed that around 80% of medtech companies had experienced a cyberattack in the past five years. But only 13% reported being 'very prepared' to mitigate future attacks. Although this offers a big opportunity for hackers to invade systems, it offers an even bigger opportunity to make great strides in the detection and protection against them.

Covid-19 also caused a vast increase in telemedicine: remote diagnosis, treatment and monitoring of patients to help them avoid a visit to a doctor's office, whether they are positive for Covid or not. While it was estimated that only 10-15% of healthcare services took place via telemedicine before the pandemic, it is estimated that up to 50% of healthcare is conducted via telemedicine today. And that number is only expected to grow. The telemedicine market in 2019 was estimated around US$4.9 billion. It's predicted to be around US$194 billion by 2023, and a staggering US$459 billion by 2030.

SBOM as the foundation of protection

As AI-driven medical devices and telemedicine continue to improve, they will be able to do more and unburden the healthcare system even further. But given the vast vulnerabilities in this market, mostly due to lack of knowledge about the severity and number of potential threats, medtech companies need to act now to slow the tide of cyberattacks.

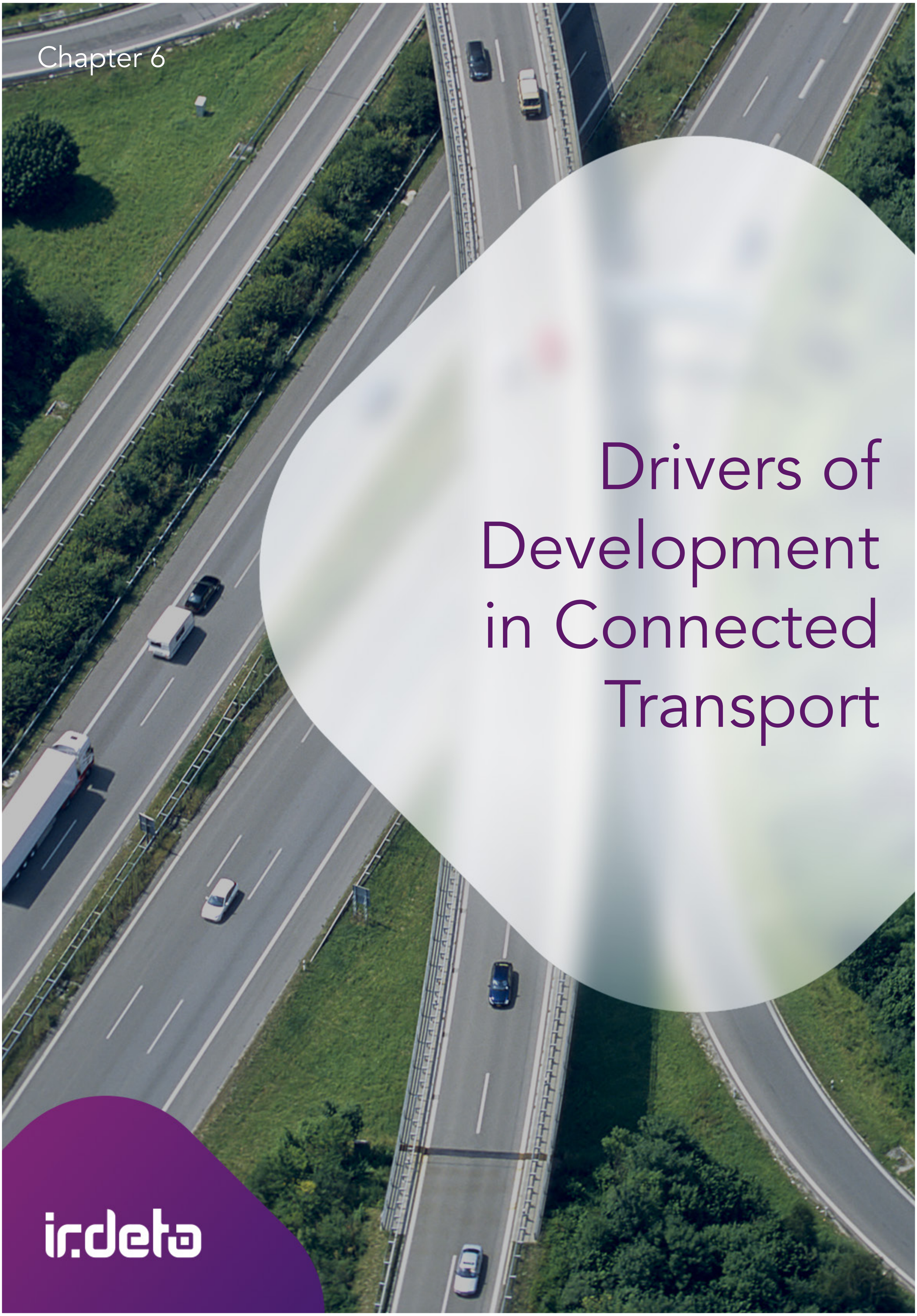
There's a significant industry push to improve the medical device game. That's why the U.S. FDA is pushing back with Software Bill of Materials (SBOM) regulations for medical devices. An SBOM is a detailed roadmap of all the companies, systems, software and materials used to make connected devices. With the SBOM secured, the medtech community can identify and proactively respond to software vulnerabilities, manage supply chain risk, ensure supply chain accountability and improve security in the short and long term.

Security from the start

The SBOM is a significant and powerful tool in the fight to protect medical devices from attack. But medtech must do even more. It all starts with robust threat modelling to uncover vulnerabilities and weaknesses. Then, the implementation and validation of sufficient threat cover during the device design phase. Once the device is released and in use, the SBOM will enable complete understanding and traceability of software, and will indicate which threats the device may be vulnerable to, and what mitigation actions should be taken. Lastly, every device must be carefully monitored and updated over its entire lifecycle, to offer continuous protection of critical functionality and precious patient data. For example, SBOMs will enable companies to immediately see if the prolific Log4j vulnerabilities are a threat, and what to do to about them.

Healing medtech with vigilance

Given that medical devices are often used for years, and threats and attacks continue to increase, Irdeto will continue to focus in 2022 and beyond on protecting the systems that protect our health. And that means closing the gaps in medtech development and continuing to monitor telemedicine and medical devices to ensure optimal levels of protection. So that, long after the pandemic is behind us, the medical industry can continue to use technology to its advantage to improve patient care and ensure optimal efficiency. But only if – and when – we slow the tidal wave of attacks that currently plague the industry.



Chapter 6

Drivers of Development in Connected Transport

A few years down the road, when we look back at 2021, it will likely be seen as a pivotal year for connected transport. Not because of tremendous advancements in the technology of vehicles, off-highways or fleets, but because of two powerful drivers that are set to turn the entire industry on its ear. A combination of new regulations and shifting market trends are paving the way for significant advancements in connected transport security in the coming years.

Regulations that fuel innovation

Research shows that 775 million consumer vehicles will be connected by telematics or apps by 2023. And transport fleets, public transportation and logistics chains are all embracing connectivity as the key to efficiency. But with all that connectivity comes a vast increase in the number and variety of potential cyberattacks.

But the cavalry is on the way. The adoption of UNECE's WP.29 Cybersecurity regulations in 2020, and ISO/SAE 21434 and the European NIS2 in 2021 are driving connected transport strategies around the world. This has a direct impact on the specific challenges that OEMs want to solve. It also positively shapes the way Irdeto brings our relevant technology and expertise to the market.

Rolling towards solutions

The adoption of regulations has dominated the past 18 months. Their implementation will dominate the next 24-36 months. In most relevant industries, cybersecurity can't change overnight. Meaningful change happens throughout an organization, not in a single isolated department in the basement.

Today, the market needs trusted partners who understand the industry well and can navigate the complex world of cybersecurity, regulation and defense on their behalf. It has become more and more challenging to address specific segments and markets with broad or horizontal cybersecurity technology. The needs and challenges are becoming increasingly industry-specific, and as such require a deep understanding of those industries to properly address them.

Irdeto continues to more closely align ourselves within the most relevant segments in the connected transport space. Fleets, Off-Highway Equipment, and Rail are the first areas of increased focus, and as we grow, we improve both the depth of our segment knowledge and the breadth of our underlying cybersecurity technology.

Consumer trends that accelerate development

The second major shift in the connected transport space is the increased demand for customer-centric solutions. Car makers can no longer differentiate based on vehicle performance, reliability, efficiency or other technical and mechanical characteristics of their fleet. Today's consumer wants comfort, convenience, and connectivity. Built-in navigation and entertainment features, automated maintenance monitoring and state-of-the-art security, among others. Even more is expected from electric vehicles, which require close monitoring and constant updates to reduce latency and improve performance.

In a fiercely competitive industry, this consumer push is driving OEMs to expand their connected services and focus on customer desires. Several major manufacturers have even added a Customer Experience Executive (CXO) to their C-Suite. But no matter what, if manufacturers want to compete in the connected transport era, they'll need a security partner that can ensure that the comfort and convenience that customers want, doesn't come at the cost of the security they need. As in any other industry, serious security breaches or hacks can not only be financially devastating, but also destroy an OEM's brand and reputation.

The roadmap to success

So, what does effective security for connected transport look like? In 2022 and beyond, OEMs should focus on a number of key development areas. First and foremost, threat modelling and mitigation should be the starting point of any new innovation. Second, security-by-design principles should guide each and every development process. And systems need to be implemented to ensure constant software monitoring and updating to prevent future attacks. Certain AI technologies can even add new levels of vehicle security, such as by requiring multi-factor authentication in the event of abnormal activity within the vehicle. So, if a hacker clones the car key, the vehicle will 'know' to verify the driver's identity before allowing the car to start.

For Irdeto, 2022 is shaping up to be the first year in a new era of connected transport protection. Our more than 50 years of cybersecurity expertise, combined with our deep understanding of the specific challenges OEMs face, and our ability to identify, monitor and eliminate threats to connected transport is nearly unmatched in the industry. As OEMs turn their focus to complying with regulation and satisfying consumer demand, Irdeto will continue to apply our expertise to develop custom-made solutions for OEMs' unique challenges.

Come what may, Irdeto will be here

While the current cybercrime landscape may seem daunting, customers can take comfort in the fact that Irdeto has been part of the fight for more than half a century. We bring all the power of that experience to bear every day, and continuously renew our systems and services to protect our customers' most valuable assets.

And in the years to come, Irdeto will continue to develop into a full-service protection and defense partner, addressing all of our customers' needs with precision, dedication, and endless vigilance. We will be where the criminals are, and keep an unblinking eye on every new development. We will work with regulators and governments to further tighten the reins on cybercriminal activity. And we will create innovative solutions to the most challenging security questions of the day.

Our customers trust Irdeto because we have earned that trust. Through decades of success, by changing with the times, and by growing our skills every time the bad actors grow theirs. Our pledge continues to be to offer the most robust and extensive protection possible. We won't back down and we won't rest until we empower people to utilize the power of connectivity without the threat of invasion.

Last modification: 27-01-2022 / 10:33 am GMT+01:00