ecosystm

SUPPORTING PARTNER

SGINNOVATE

ECOSYSTM PREDICTS

The Top 5 Cybersecurity & Compliance Trends for 2020

AUTHORED BY:

Carl Woerndle, Claus Mortensen and Alex Woerndle

This report presents Ecosystm's outlook for Cybersecurity and Compliance in 2020 and the associated implications for tech buyers. The predictions are drawn from the findings of the global Ecosystm Cybersecurity Study and is also based on qualitative research by the analysts.

PRESENTED BY

Team Ecosystm

PUBLISHED

November 2019

Contents

Figures

Executive Summary

Cybersecurity will remain an important topic of discussion on the world forum. 2020 is predicted to see an increasing number of state-sponsored cyber-attacks especially on utilities and public infrastructure. Eventually countries across the globe - more so the NATO members - will be forced to retaliate to these attacks. Irrespective of whether these countries retaliate, Cybersecurity will become part of an important geopolitical conversation and will impact tech buyers, consumers and tech vendors alike. This will play out against the backdrop of data compliance reforms that most countries have either embarked on or are actively contemplating.

This report presents the top 5 Ecosystm predictions for the Cybersecurity and Compliance market in 2020. It is based on the latest data from the global Ecosystm Cybersecurity study, that is live and ongoing on the Ecosystm platform.

The Top 5 Cybersecurity & Compliance Trends for 2020

API VULNERABILITIES WILL BECOME A MAIN HACKER TARGET

Industry analysts and vendors alike have spent the last couple of decades advocating the abolition of data silos in the organisation. Siloed data, while inherently more secure, is usually not accessible to the majority of the organisations' users, who might find it useful. So, companies have spent vast amounts of time, effort and money on making data and platforms available and accessible across systems and applications. It is therefore no surprise, that most companies by now are managing a vast number of APIs providing access and insights from both internal and external data. And as companies and services continue to go online, mobile and to integrate across apps and across social media, this number will only increase in the years to come.

The problem with APIs is that they are inherently insecure. APIs are about granting access to and providing transparency for developers. Client-side developers usually need fine-grained access to services and data and API documentation thus often provide great transparency on how that can be done. This is great for developers but, unfortunately, also for hackers. We have already seen several high-profile API breaches and announced API bugs. In October 2018, Google had to shut down Google+ after an API bug exposed details for over 500,000 users. In December 2018, Facebook announced that a bug in one of their APIs allowed more than 1,500 third-party apps to access private images of up to 6.8 million users. Other examples include Panera Bread, USPS and several more.

We believe the problem will get significantly worse in 2020, with API attacks quickly becoming one of - if not the most - frequent target for hackers.

Implications

Supply chain risk is not a new topic or prediction. However, the mode of attack will focus more and more on the communication layer between applications. It is almost impossible for organisations to track where and how their information flows. Responsibilities for securing, monitoring, responding to incidents, and understanding the source and traversal of breaches will be ever more complex. As a result, why would a hacker not target this grey area, enabling longer, broader and deeper infiltrations?

Securing the software development lifecycle therefore must gain more attention in 2020. The communication

link between systems, applications and organisations has traditionally come with an inherent trust that the developer of the API has processes in place to develop a secure solution. But many of these developers are small organisations with limited resources and security controls and as a client, you cannot take for granted that they take care of security.

OPERATIONAL TECHNOLOGY (OT) SECURITY WILL CONTINUE TO LAG IN 2020

Operational Technology (OT) refers to the hardware and software used to monitor and sometimes manage how devices that run on an organisation's infrastructure perform. Traditionally, OT was used for industrial control systems (ICS) - especially for critical infrastructure. The monitored devices that OT managed were not networked, and the main security focus was on physically securing the device. As devices have become smarter and increasingly network-centric, the need for integrating OT and IT has become bigger, and the threat landscape for OT has changed completely.

Many of the current OT systems were never designed for remote accessibility and certainly not for Internet connectivity and if these systems are now forming part of new IoT-based systems, they can prove to be extremely vulnerable.

We believe that OT breaches will become much more prevalent in 2020 and beyond. Still, the focus will remain on data breaches - the much-needed investment in OT security will continue to lag. This will create a 'security debt' over coming years for those that do not invest in preventative controls now.

Implications

Regulatory focus is primarily centred on privacy (data breaches) and therefore focus on security controls remains on avoiding an embarrassing breach. Investment, naturally, continues to flow to IT security. OT security has always lagged behind and it is no revelation that this will continue into 2020 and beyond. While privacy breaches remain the focus, OT vendors continue to fly under the radar and therefore have not invested sufficiently in product development to meet the security risks of 2020.

There are significant OT networks in critical infrastructure, government and traditional industry that simply cannot be defended from modern threats. This ongoing lack of investment by the OT vendors but also the buyers of those technologies only creates further security debt that, if not managed soon, may create the security equivalent of a financial meltdown.

AI TRAINING WILL RECEIVE ATTENTION FROM REGULATORS AND THE PUBLIC AS A POSSIBLE INFRINGEMENT OF PRIVACY

All the large vendors have spent considerable effort and money on developing AI in recent years. While most of these efforts have been on developing the platforms, the last year or so has seen a shift in effort towards training of AI interfaces. As players such as Amazon, Google and Apple are trying to win over consumers in home and personal assistant services, AI training - particularly in natural language processing (NLP) - has garnered a lot of attention in 2019.

Especially noteworthy was the news that Amazon's Alexa was eavesdropping on its users, with Amazon keeping a copy of everything Alexa records after it hears its name. Apple's Siri and Google's Assistant, by default also

kept recordings to help train their AI although Google later announced that they were changing that policy. Apart from the initial consternation in the press and on social media, nothing much seems to have happened from a regulatory perspective - perhaps because US politicians have been preoccupied with other pressing issues and because Alexa is still mostly an US product. This implies that EU scrutiny is still lagging.

However, this appears to be changing and US lawmakers have initiated the first steps in Congress towards a more formal scrutiny. In Europe, the privacy regulator in Luxembourg, where Amazon have their European headquarters, is reported to be scrutinising Amazon in the light of the General Data Protection Regulation (GDPR).

We believe that 2020 will be the year when AI training relying on consumer data will start to become regulated. We also believe that we may see the first serious class-action lawsuit in the US against one or more of the home automation and personal assistant providers.

Implications

For consumers and companies alike, the implication is clear: if you rely on data assistants - especially those that rely on NLP - be sure to read the fine print in the Terms of Use. If you believe that there is a real risk that sensitive data might be leaked through these devices and services and that these risks outweigh the benefits of using these services, think again before using them.

For the vendor landscape, expect the “good old days” to be over in 2020. While US regulation may or may not be introduced in 2020, we have little doubt that regulators and watchdogs in the EU will take action under the umbrella of the GDPR.

While this smorgasbord of “free access” to user-generated data may no longer be available in 2020 and beyond, vendors still have ways of training their AI platforms without necessarily infringing upon consumer rights. Google may have shown the way forward with their “Federated Learning” initiative that allows Google to train AI models on mobile devices and then transfer those learnings back to a central AI data centre. Only the learnings are transferred back - the underlying data does not need to leave the device.

Although many questions remain about how well Federated Learning will protect user privacy, it does promise a way to have the best of both worlds: insights from data as well as data privacy.

MAJOR GDPR FINES IN 2020 WILL FORCE MNCS TO INVEST IN SECURITY COMPLIANCE

Even though the GDPR came into effect more than a year ago (in May 2018), we still have not seen huge amounts of fines being issued in the EU. Even though GDPR guidelines were released to guide regulators and watchdogs of the individual member countries, these entities still had to work out their own frameworks and policies on how to enforce the regulation. However, they are finally getting there. While we only saw two fines issued in 2018, at least 17 were known to be issued in the first half of 2019, totalling about EUR 52 million. In the third quarter of 2019, at least 12 fines were issued totalling about EUR 328 million.

We believe that the trend is clear: Expect to see a magnitude of companies across EU be penalised in 2020. We should also expect several fines above EUR 100 million.

Implications

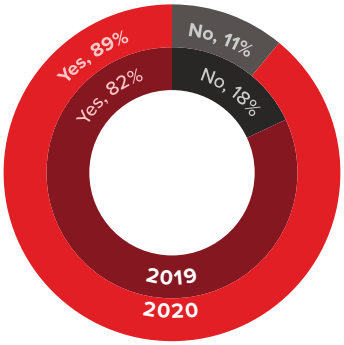
This is unlikely to directly affect companies outside of the EU - especially in Asia - who do not have any representation inside the EU (even though they perhaps should, according to the GDPR). We do not expect any fines issued to or indeed collected from companies outside the EU but falling under the purview of the GDPR.

However, increasingly the global scope of the GDPR will make it harder and harder for companies to ignore or escape the impact of this regulation. Consequently, we expect to see increased spending on GDPR compliance in the areas of IT security, privacy and data management in 2020 and beyond - even outside the EU.

MERGERS & ACQUISITIONS WILL RATCHET UP SIGNIFICANTLY IN 2020

Mergers and Acquisitions (M&As) in the Cybersecurity sector is nothing new, but we expect a significant uplift in activity in 2020 as a range of factors combine. Like the consolidation activity in previous booms (such as digital media and web services in the early 2000s), Cybersecurity is booming globally and therefore creating opportunities for cashed up vendors and private equity. This will in part be driven by organisations' desire to interact with one vendor for all their Cybersecurity requirements and a shift towards managed services. The Ecosystm Cybersecurity study reveals that organisations engage managed security service providers (MSSP) for their deployments (Figure 1).

Figure 1: Use of MSSP for Current and Planned Cybersecurity Deployments



Source: Ecosystm, 2019

N=1,379

The fragmented security market has thousands of vendors and consultancies globally. Every day a swathe of new start-ups announces their ground-breaking new technology. Coupled with significant investments globally in tertiary education and industry certifications for a growing workforce, the next generation of Cybersecurity entrepreneurs are entering with force.

We believe that this creates both threats and opportunities for the cashed up established Cybersecurity providers that need to remain innovative and growing.

Implications

Industry M&As will be larger, bolder and much more regular in 2020 as 'FOMO' - fear of missing out - takes hold. We will see some of the smaller firms seeking divestments to the established players as their ability to gain an audience with buyers gets more difficult in a very crowded sector. All combined, we have a sector ripe for significant growth in M&As. However, the only winners may well be the investment bankers rather than the industry participants - particularly tech buyers.

The security market is shifting towards managed services. Small vendors are seeing an opportunity to merge their technologies into MSSP providers, providing scale and diversity of income streams. Emerging MSSPs in turn are looking to consolidate market share through acquisitions in a race to the top. As the demand for managed services grows, driven by a need to shift CapEx to OpEx, the market will see a growing number of M&As as MSSPs acquire vendors to lock down the better technologies for themselves.

This report is based on the analysts' subject matter expertise on the area of coverage in addition to specific research based on interactions with technology buyers from multiple industries and technology vendors, industry events, and secondary research.

The data findings mentioned in all Ecosystm reports are drawn from Ecosystm's live and ongoing studies on the Ecosystm research platform. This report refers to data from the global Ecosystm Cybersecurity Study based on participant inputs that include decision-makers from IT and other Lines of Business, from small, medium and large enterprises.

For more information about the Ecosystm Cybersecurity Study and other research topics, visit www.ecosystm360.com.

About Ecosystm

ecosystm

Ecosystm is a private equity backed Digital Research and Advisory Platform with global headquarters in Singapore.

As a global first, Ecosystm brings together tech buyers, tech vendors and analysts into one integrated platform to enable the best decision making in the evolving digital economy. The firm moves away from the highly inefficient business models of traditional research firms and instead focuses on research democratisation, with an emphasis on accessibility, transparency and autonomy.

Ecosystm's research originates from its proprietary "Peer-2-Peer" platform allowing Tech Buyers to easily benchmark their organisation, while providing Tech Vendors with access to real-time Market Insights in an affordable "as-a-Service" subscription model.

About SGInnovate

SGINNOVATE

At SGInnovate, we build and scale Deep Tech startups into high potential companies with global impact. We believe that hard global problems can be solved using Deep Tech, and Singapore, where we are based, is uniquely positioned to realise Deep Tech innovations that can tackle these challenges. Our Deep Tech Nexus Strategy is focused on adding tangible value to the Deep Tech startup ecosystem in two key areas – development of Human Capital and deployment of Investment Capital. With the support of our partners and co-investors, we back entrepreneurial scientists through equity-based investments, access to talent and business-building advice. Our efforts are prioritised around emerging technologies such as Artificial Intelligence, Autonomous Tech, MedTech and Quantum Tech, which represent impactful and scalable answers to global challenges. SGInnovate is a private-limited company wholly owned by the Singapore Government. For more information, please visit www.sginnovate.com