STRATEGY / INSIGHT / TECHNOLOGY

infosecurity

State of Cybersecurity Report

FEAR AS A CYBERSECURITY DRIVER

AI AND AUTOMATION

GDPR AND LEGISLATION

infosecurity

STATE OF CYBERSECURITY REPORT

Authored by Dan Raywood

It is important to determine what is pushing cybersecurity forward, what the future of cybersecurity looks like and whether the industry is healthy and growing at the rate it should be. In this inaugural report, *Infosecurity* undertook a research project to determine the answers to those questions, and establish what the main drivers are for cybersecurity spending and behaviors now and in the next five years.

Infosecurity interviewed 32 leading information security experts on what they thought were the current main drivers in the sector. A number of subjects were proposed, with the following proving to be the most common:

- GDPR and regulation (46% of respondents)
- The expanding threat landscape and evolving attacks (34% of respondents)
- Greater board level recognition of cybersecurity as a business risk (21% of respondents)
- Use of the cloud (21% of respondents)
- Selling via FUD and panic (18% of respondents)

The Introduction of GDPR and Increased Regulation

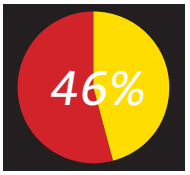
Increased regulation was the most cited driver for cybersecurity, and for good reason, as the GDPR has proposed the greatest change in data protection law for the online age, bringing with it a variety of impacts on the industry. Ed Tucker, CIO of DP Governance, said that regulations like GDPR are "again bringing information and cybersecurity out of the dark corner and into the business."

In a 2017 Watchguard Technologies survey of 1600 organizations, 37% of respondents claimed they did not know whether or not their company needs to comply.

Consultant Neira Jones said that GDPR, as well as the revelations around Facebook/Cambridge Analytica, have had a significant impact on business models and will continue to drive technology innovations not only in the technology space, but also in the governance space.

Jones added: "The GDPR is putting mitigation technologies such as encryption, tokenization and anything under the banner of anonymization/pseudonymization very firmly into the public consciousness."

Our research also revealed a common theme that GDPR could have an impact on other regulations. Savage Security consultant Adrian Sanabria said that he could see GDPR's impact reflecting that of the debut of the Payment Card Industry Data Security Standard (PCI DSS) almost 13 years ago.



46% of respondents believe GDPR and regulation is driving cybersecurity spending and behavior

"Version 1.0 of the PCI DSS went into effect in October 2005 and it had a profound impact on the security industry," he explained. "Many pointed out that, because the PCI DSS was so prescriptive, it 'chose' winners and losers in the marketplace. In fact, the original version of the DSS mentioned Tripwire by name, acting as an implicit endorsement that launched the company's growth as a result. The success of the SIEM, penetration testing services, IDS/IPS and WAF markets were also spurred by PCI requirements."

Jones said: "The other main regulation to look at is the second Payment Services Directive (PSD2), which is driving authentication solutions, especially multi-factor and biometrics, compounded with the fourth Anti-Money Laundering Directive, which is also driving KYC developments (and therefore going back to identity and authentication), which in turn circles back to information/cybersecurity with the black market flooded with stolen

credentials. In addition, as PSD2 drives Open Banking, we can expect that API security will become an area of focus."

Ovum research director Maxine Holt, pointed out that compliance is a huge issue right now for organizations, because along with GDPR, there is also the Networks and Information Systems (NIS) Directive.

In a survey by GlobalSCAPE and the Ponemon Institute, 90% of respondents considered GDPR to be the most challenging among other data compliance regulations.

What about how GDPR is driving the overall business agenda? Steve Durbin, managing director of the Information Security Forum (ISF), said that such legislation "is helping to put cybersecurity on the risk agenda" and is ensuring that the conversation about the need to understand and effectively manage the cyber-risk profile is taking place at the right levels in organizations.

Tom Salmon, financial services specialist customer engineer for Google Cloud Platform, said that there is a GDPR challenge around determining where and what data is, and whether it is sensitive. "If you have a database in various places, is it your liability to hold onto it? If you can't protect it, then don't collect it," he argued.

> ***"People will have to realize that their data is currency and it is a handler's responsibility to protect it"***

This reflects one of the main challenges of GDPR compliance: understanding where data is, and how it is secured. Also, Phil Dunkelberger, CEO of Nok Nok Labs, felt that despite there being plenty of regulations that state a company is required to take 'due care', situations arise where data is misused.

"People will have to realize that their data is currency and it is a handler's responsibility to protect it. It's been taken advantage of for years and it will continue to be."

That level of compliance will drive cybersecurity forward in a direction of good practice around data protection. However, the headache of achieving compliance could well come with a hangover of how securely you are keeping customer data and the ways in which data could leave the perimeter.

The Expanding Threat Landscape and Evolving Attacks

Whilst protecting data is one challenge, defending it from attackers is quite another. Those we surveyed determined that increased tactics used by attackers was a genuine driver for cybersecurity, with comments received on the scalability of machine learning used for malicious purposes, whilst others cited an increase in the size of DDoS attacks and ransomware capabilities as the biggest threats.

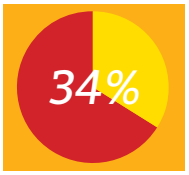
According to the Online Trust Alliance's *Cyber Incident & Breach Trends Report*, ransomware usage resulted in 160,000 cyber-attacks in 2017 – double the amount (82,000) in 2016.

Gregory Parfitt, application security specialist at the Trainline, said that high-profile incidents and breaches were the main driver of cybersecurity, particularly with the breach at Experian and the ransomware incident at FedEx, whilst DDoS attacks measured at 1.4 Tbps were driving the defense of security.

According to Corero research in April 2018, 91% of 327 security professionals said that individual DDoS attacks can cost their organization up to $50,000 in terms of lost business, and 69% indicated that their organization experiences between 20-50 DDoS attack attempts per month.

Other comments also determined that there are a variety of threats, including nation state attacks, affecting UK business of all sizes. Tim Ward, director of Think Cyber Security, warned that even the smallest of businesses are starting to affected by threats such as spear phishing, though they are often uncertain about what to do due to budget and knowledge constraints.

Consultant and author Raef Meeuwisse said that the rapid evolution of the cyber-threat landscape was "without doubt the main driver for change" while principal consultant Nick Drage added that it was about the ability to improve detection and response capabilities, rather than trying to prevent attacks. "While this has been the recommended way forward for years, I think a lot of organizations are still getting to grips with it," he explained.



34% of respondents believe the threat landscape and evolving attacks are driving cybersecurity spending and behavior

Maxine Holt claimed that the problem with attacks is in trying to stop them, as attackers will always look for new opportunities. "As zero-day vulnerabilities reduce, threats will try their luck at any and every opportunity to compromise an organization, e.g. through cryptojacking, using the supply chain to deposit malicious payloads, and so on."

An argument around cybersecurity attacks and defense has been that the adversary has always had the upper hand, and only needs to be successful once whilst defenders need to be constantly ready. Scott Crawford, research director of the information security practice at 451 Research, said that cybersecurity is ultimately an asymmetric contest, as the adversary can focus on any opportunity they wish, using any combination of tools as deliberately as they choose.

"The defender, on the other hand, must make the best use of limited resources to defend the entire attack surface as best they can. How they make those decisions has been a key driver in everything from risk management to the embrace of modern analytics to better recognize and respond to threats."

Defending against an ever-persistent threat remains a consistent challenge in cybersecurity, and for that reason the arguments about defense remain prominent. However, a decent attitude towards cybersecurity in the business could enable a better defense, but is cybersecurity really being recognized at all?

Security Not Recognized as a Part of the Business

Is cybersecurity being recognized by the board, and if not, can cybersecurity even be a driver for a business? Whether or not cybersecurity is something that the board can recognize as a genuine business risk has been questioned for some time and according to survey responses, this is a continuing driver.

Brian Honan, CEO of BH Consulting, said that "better awareness at board level about cybersecurity and seeing it as a business risk and not an IT risk only" was a key driver, whilst Andy Samsonoff, CEO of invinsec, believed that "IT security is still seen as a niche or largely technical activity" and not something that most staff need to worry about.

"Businesses that take this approach put themselves at greater risk of security and data breaches," he said. "Whereas

those that bring their CISO into the center and empower them across the whole business are the ones that, in the long term, will suffer less and spend less. Security issues can often be dealt with far quicker by incorporating information security into the discussion early on and by holding commercial P&L holders accountable for the security of their business areas."

Whilst this is dependent on the company, it may be the case that there is no CISO in an organization at all, or that they report into a person such as a CIO or a CEO who is on the board.

Dr Jessica Barker, co-founder of Redacted Firm, said that with more and more cyber in the news, more people are talking about it, and it is increasingly in front of boards "who want the team to tell them what they are doing," in order that the management knows how the business is affected.

According to Osterman Research from 2016, only two in five IT and security executives feel that the information they provide to the board is actionable, and even fewer believe they are getting the help they need from the board to address cybersecurity threats.

Is it the case then that boards are more actively interested in cybersecurity issues, and after the major headlines of 2017 they cannot avoid the major stories and instances of CEOs being held to account?

David Shrier, CEO and founder at Distilled Analytics, said that corporations have not allocated sufficient resourcing to support cyber-efforts that are relative to the magnitude of the risks they are now facing, while Pinsent Masons CISO Christian Toon argued that demands on responsibility for data was waking up businesses who "would not do business with organizations that cannot demonstrate good controls or practices."

Toon also claimed although large breaches at TalkTalk and Equifax did not kill those businesses, it has been hard for them to regain trust. "Security roles across the industry feel the reputational pressure, and I see CISOs walking into organizations that take it seriously and away from business which do not," he said.

Research from 2016 by Bay Dynamics found that two in five respondents felt the information they provide to the board is actionable, and only one-third believed that the board understands the information about cybersecurity threats that is provided to them.

Part of the problem may be that boards see the hype that so often surrounds cybersecurity, rather than the genuine risk that a business is facing in 2018. This leads us to our next topic, which could be the reason why cybersecurity is not being taken as seriously as it should be.

Selling Via FUD and Panic

As an industry that has had a heavy reliance on marketing and communications to get the message straight and communicate in the worst times, there has also been an element of selling on the concept of 'fear, uncertainty and doubt', or FUD, as it has become known.

In those instances where FUD is used to sell, respondents claimed that there is a "culture of fear" commonly used to sell security. Andrew Henderson of Wychwood Consulting and secretariat of the All-Party Parliamentary Group on Cyber Security, said he felt that there was "a general climate of fear in the media," with Ed Tucker adding that although "global coverage of cyber-events" is sometimes "overhyped," the coverage does bring "cyber more and more to the fore, and beyond just a security team conversation."

This culture of fear is seen as a negative tool. Jothy Rosenberg, founder and CEO of Dover Microsystems, said

that this creates confusion as "no one seems to know what to do. Everyone is just throwing anything at the wall to see what sticks." Rosenberg also said that when fear is used to sell, "the current spate of solutions available aren't enough to stem the tide."

If this is a driver for cybersecurity, perhaps it is the case that the problem is actually more about hype? Ian Levy, technical director of the National Cyber Security Centre (NCSC), said that he would like to see cybersecurity "democratized" and be determined as another business risk, and to do that we need to "get rid of the hype."

"What is driving cybersecurity now is fear, and as a community we don't talk in the right way to help people make responsible decisions," he added.

There is a need for better communication, and perhaps this could lead to a more mature acceptance of cybersecurity at all levels, if the FUD is rubbed out.

Use of the Cloud

The final driver that was most frequently raised related to the use of the cloud and hosted services. Whilst the conversation on whether the cloud is secure or not has faded somewhat over time, there remains some skepticism about data protection – relating back to the first driver. However, the offer of cloud has become commoditized due to the emergence of Infrastructure-as-a-Service (IaaS) offerings from Microsoft Azure and Amazon Web Services (AWS).

> ***"There is better awareness at board level about cybersecurity and seeing it as a business risk and not only an IT risk"***

Adrian Sanabria said that cloud has been a persistent trend for a while, but we've reached a point "where a lack of discipline and best practices are coming back to haunt us."

"The cloud is still one of the easiest places to secure data and applications, but like encryption, there is a limited pool of individuals skilled and experienced enough to implement things properly. We've now seen dozens of high-profile breaches due to improper access controls on AWS S3 buckets alone. Also, like encryption, the cloud is as unforgiving as it is powerful," Sanabria explained.

In agreement were consultant Robert Schifreen – who added that more users need to realize their responsibility for the security of data when it is hosted by a cloud provider – and analyst Bob Tarzey, who said that cloud was a driver for cybersecurity "both as a cause of concern and as a way to ensure better security."

Nick Drage argued that it has taken a long while for organizations to adopt cloud and realize the security benefits and cost savings of cloud platforms over on-premise, and to appreciate the security expertise of cloud providers over in-house talent.

According to the *2018 Cloud Security Report* from Crowd Research Partners,

90% of cybersecurity professionals are concerned about cloud security, with the main worries surrounding data loss and leakage (67%), threats to data privacy (61%) and breaches of confidentiality (53%).

Also, according to the 2018 *Oracle and KPMG Cloud Threat Report*, 41% of respondents employed a cloud security architect.

The use of cloud brings its own management and skills debates, and Tom Salmon claimed that while every company is different and multiple platforms can be hard to monitor and require different skills, using the cloud does require more than just "taking a firewall and putting it in your cloud provider."

Issues such as cloud show that there are persistent drivers over a number of years rather than things that are especially new or groundbreaking, and new IaaS developments show that this has been a serious game changer for cybersecurity whilst embracing a significant change.

These five aforementioned drivers were the most common among our respondents, and other drivers that were also noted included: AI, ransomware, security of the perimeter, IoT and DevOps.

In the next section, we will look ahead and analyze the responses on what will drive cybersecurity into the future with specific focus on the next five years.

The Future

In terms of what will drive cybersecurity into the next five years, the perspectives were even broader, but the most common topics were as follows:

- GDPR and future legislation (34% of respondents)
- Greater use of cloud platforms (34% of respondents)
- Adoption of AI and automation technologies (28% of respondents)
- Increased creativity of attacks (28% of respondents)
- Increase in IoT (25% of respondents)
- Better ability to hire and provide mentoring (18% of respondents)

Adoption of AI and Automation Technologies

The concepts of automation and artificial intelligence have taken over the cybersecurity headlines in the past couple of years, so it is not a surprise that this is deemed to be a major trend going forward. The general consensus was that there will be a greater adoption across the security practice, and that these tools may be more effective in combatting attacks.

Scott Crawford said that analytics have become pervasive throughout the security technology market, but "we are still yet to see true AI have an impact on automating the mitigation of risks more consistently across the attack surface."

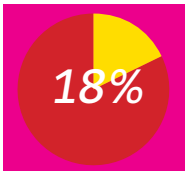
Crawford added that we will likely see machine learning or AI applied to studying and exploiting weaknesses in a potential target, too. "As computing becomes increasingly pervasive and 'smart' devices, endpoints and heretofore physical systems embrace IoT technologies, that could greatly expand those opportunities for the attacker," he said.

Adrian Sanabria was also skeptical, saying that automation and orchestration could have a big impact on information security, but it is far from certain at this point as "this is another new skillset for most businesses."

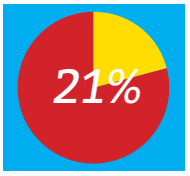
He claimed that the challenge is for security teams to get comfortable enough with automation and orchestration to be able to deploy it broadly. "If these challenges are overcome, the automation trend could alleviate some of the staffing challenges the security industry is currently suffering from," he argued.

According to research by Radware, four in five (81%) respondents reported having already or recently implemented more reliance on automated solutions, whilst

> ***"Those that bring their CISO into the center and empower them across the whole business are the ones who, in the long term, will suffer less and spend less"***



18% of respondents believe that selling via FUD and panic is driving cybersecurity spending and behavior



21% of respondents believe that cloud is driving cybersecurity spending and behavior

57% of executives admitted to trusting automated systems that employ AI and machine learning as much or more than humans to protect their organizations.

Andrzej Kawalec, CTO and head of strategy and innovation for Vodafone Enterprise Security, believed that the heightened cyber-risk profile for many organizations, when compared to a worsening cyber-talent situation, will drive huge changes in the use of operational cyber-automation and AI to deal with the capability gap facing all cyber-teams.

The consensus on AI seemed to bridge two gaps – the lack of people and the need to meet the demands of threats and alerts. Mark Weir, director of cybersecurity, Cisco UK & Ireland, said that the implementation of emerging technologies like AI, machine learning and automation will "make it increasingly difficult for cyber-criminals to impact our lives."

> ***"There is a limited pool of individuals skilled and experienced enough to implement things properly"***

For Chris Payne, managing director of Advanced Cyber Solutions, the general trend of automation was the main driver for cybersecurity in the future, whether it be for decision making or system interoperability.

Security solutions, and other IT systems, are producing huge quantities of analytical data which has the potential to produce risk reducing decisions," he said. "This AI-style trend will continue to self-protecting networks and systems."

It is easy to see how and why AI would be the most popular driver for the future of cybersecurity: it is a popular topic now, and its benefits do seem to outweigh the negatives in terms of what it can offer. However, the potential problems involve the amount of human input required to configure such technologies so they work efficiently, and the faith in being able to deal with alerts – not to mention the 'Skynet' factor, and putting all of your faith in a machine.

Increased Creativity of Attacks

Much like the current driver of attack capabilities increasing, the evolution of cyber-attacks will drive cybersecurity forward in the future because of the need to defend against an ever-increasing adversary who has the drive to succeed.

Adrian Sanabria said that the shutdown of botnets forced attackers to shift tactics, which resulted in ransomware and once ransomware is stopped, he questioned whether we will be ready for the next shift? "I doubt it," he said. "We tend to think only one move ahead. We need to be playing this like a game of chess, thinking several moves ahead."

So what kind of attacks could we expect? Tim Ward predicted that there may be some genuinely significant targeted state-sponsored attacks with "kinetic" outcomes, while Bob Tarzey warned that there will be the ability for cross-organizational business processes to be disrupted via cyber-attacks.

Reflecting on cybersecurity in the past five years, Canon Europe director of information security Quentyn Taylor pointed out that although threats such as business email compromise have been possible for years, greater automation of phishing to enable account takeover is a driver for the future of attacks.

"The Blaster and Slammer worms had more impact than NotPetya as that impacted online processes, but in the future no one can be offline and so taking a business offline with an attack in five to 10 years' time will be more devastating as there is a dependence on being online," he said.

According to the NCSC first year threat report, between October 2016 (when the NCSC was opened) and the end of 2017, it recorded 34 "significant" cyber-attacks like WannaCry which required a cross-government response, and 762 less serious incidents.

So if increased attacks and attackers' capabilities are a future driver for cybersecurity, is it actually an especially negative future for businesses? Generally there did seem to be some positivity in the responses.

Andrew Henderson predicted a better understanding about how the criminal market actually works, while Mark Weir said that increased collaboration across all industries, and constant innovation, will make it increasingly difficult for cyber-criminals.

Raef Meeuwisse felt that major cyber-incidents "are most likely to trigger improvements in security investment" as no enterprise wants to be caught out a second time by the same threat.

Cyber-attacks are arguably what drives innovation forward in security: when an attack is stronger, the defender has to be better and this is what creates a more agile and dynamic defensive posture. As long as attackers are after something, that will have the effect of driving cybersecurity forward.

GDPR and Future Legislation

Even though the deadline passed in late May, GDPR will be a barometer of future data protection legislation and as we discussed earlier, there are other regulations which have been passed which will help put cybersecurity on the risk agenda – such as the NIS Directive and PSD2.

From the responses we received, it did seem that GDPR would create a more theoretical challenge: Andrew Henderson determined this to be the main driver; as it catches on and is understood, it will change people's perception of information security.

Gregory Parfitt agreed, saying that legislation, and specifically GDPR, will have a massive impact on how businesses look after customer data and systems for choice and preferences. He also predicted that the development of new industry standards and updates to what is existing, such as ISO27001 and Cyber Essentials, will "ensure the web is safer and get people to look twice and make better decisions."

Brian Honan said that as cybersecurity is seen more and more as a business risk, businesses will have to improve their security due to pressure from regulators and also from insurance providers. "Managing cybersecurity and data protection will become part of a business' day-to-day operations similar to health and safety, equality and accounting compliance."

Vulnerability analyst and COO of the Women's Society of Cyberjutsu Mari Galloway, said that the biggest driving factor will be legislation, and getting the right people in the room to develop and implement legislation will be key.

"Allowing the industry experts to add input will also be key," she continued. "Innovation will also drive change. We have innovation now but taping into the next generation of cyber-ninjas will


GDPR
25 May
2018
Shift

provide different perspectives on implementing better security measures."

It seems that rather than the scramble to comply with the May 25 deadline provided, the future of legislation will be driven by the demands of consumers for businesses to be better at protecting their data. Dr Jessica Barker said that the more demands from consumers and the more that they think about accessibility and availability, the "more they will vote with their feet."

While GDPR may be seen as 2018's regulation, it will change other legislation in the future as more emphasis is put on the consumer's interest, and more demands are put on the business. Will other regulations be changed as a result? It seems unlikely as they are probably in or under review anyway, but businesses continue to face the reality of providing better security for customer data.

Greater Use of Cloud Platforms

One such reason for greater control of data, and the need to prove the level of security, is because of the increased use of cloud services and IaaS. A number of respondents pointed to the emergence of AWS and Microsoft Azure as a changing point for IT. Gregory Parfitt said that these are becoming the "in-thing" to use, and as a result there will be a bigger focus for attacks and we need to adapt strategies to protect these solutions.

He highlighted changes in April by the PCI council that updated guidance on using them within cloud services, particularly on how there is a reliance on third parties to provide a service, but not enough emphasis or knowledge on what to do if a supplier of a supplier is hacked, and the impact if you use several suppliers.

Ruggero Contu, research director at Gartner, said that enterprises are opening up increasingly to the idea of "digitization of business." This is because of the adoption of IoT, mobile computing models and cloud computing, which can introduce a new set of risks and vulnerabilities "both directly (through corporate initiatives) or indirectly (through business partners and the supply chain). This means that security will have to adapt and expand its reach to new domains which involve the convergence of physical and logical."

While providing challenges for businesses, there are solutions too. Chris Payne pointed out the need to recover and return to service from attacks and breaches "almost immediately," and this will "fuel focus on incident response solutions, high availability in software, networks, geographical location and capacity" which surely the cloud and IaaS can provide.

If this is the challenge, what are the solutions? Tom Salmon said that Cloud Access Security Brokers (CASBs) are a solution "to a point," as when people look at using the cloud there is a tendency to use certain technologies. Gartner defines the CASB as an on-premise or cloud-based security policy enforcement point, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies and consolidate multiple types of security policy enforcement. "Yes we see people using them, but in an unsophisticated way," Salmon claimed.

> ***"We tend to think only one move ahead. We need to be playing this like a game of chess, thinking several moves ahead"***

Another option is containerization, which Raef Meeuwisse said will "substantially reduce and erode the role of network security."

He argued that network security is about securing the data, application, communications route and the device, and "most infosec experts seem to accept that you cannot allow a lot of roaming user endpoints to connect into a network and keep it secure – so I think secure networks will become just the segment where certain data is held securely."

Better Ability to Hire and Provide Mentoring

One challenge with the cloud, and also with the management of IoT and use of AI and machine learning, is the age old problem of the quantity of skilled people, and having the right number of people to deal with all of the ongoing issues.

According to the *ISACA State of Cybersecurity 2018* report, 59% of respondents reported having unfilled security positions, and 26% said that it can take "six months or more" to fill a role, whilst 25% said it can take three months. Of those surveyed, 30% said that less than 25% of applicants were "well qualified."

Several respondents to our research claimed that there needs to be a greater realization and inclusion of the human or social side of cybersecurity, whist security consultant Ben Tomhave said that "staffing challenges and the necessary move to automation and orchestration" will be the largest challenge that will drive change.

He argued that finding entry-level positions in information security will become increasingly difficult as candidates will be expected to come to the table with considerable hands-on experience in a number of technical topics ranging from coding to infrastructure management to automation and beyond.

In agreement was Quentyn Taylor, who added that in the past applicants would come with Unix sys admin skills, for example, but that is less common now. He felt that many applicants do not understand basic skills, and "a change needs to occur."

Security architect Jason Steer said that the drive for diversity will bring different and varying skills sets – which are needed – as well as a better aptitude within people.

The ISACA report found that 77% of all of those polled believed that women are offered the same opportunities for career advancement as men; however only 51% of women surveyed believed that to be the case. Also, 49% said there are no diversity programs in place to specifically support female cybersecurity professionals.

The overall problem of a skills shortage is being addressed by government initiatives like Cyber First, and industry efforts like Cyber Security Challenge, but these may take time to turn candidates into professionals. As a result, the workforce shortage will drive change and this will force businesses to explore other options in the next five years.

Maxine Holt said that increasing numbers of organizations will look to managed security service providers (MSSPs) to provide more of their security capabilities as they struggle to attract and retain security talent in-house. "This will also be driven by

increasing complexity as enterprises bolster their digital capabilities (the top priority for enterprises in Ovum's ICT Enterprise Insights for this year), which results in the threat landscape continuing to expand faster than organizations can keep pace."

Increase in IoT

The increasing attack surface can easily be blamed on the number of IoT devices now being used. Some are built securely, but the majority are not. Despite more legislation being put in place to better secure IoT devices, more and more devices offer internet connectivity which is more convenient for users to use than not.

According to a survey by Gemalto, most (90%) consumers lack confidence in the security of IoT devices, and IoT device manufacturers and service providers spend just 11% of their total IoT budget on securing their devices, and 50% of IoT companies have adopted a security-by-design approach.

A number of respondents pointed to the changing regulations around IoT. Andrzej Kawalec called the "cyber-safety paradigm, driven principally by IoT and industry 4.0 adoption" as the most profound change that we see on the horizon, while Phil Dunkelberger named IoT and machine-to-machine as the main driver, but asked the key question on who is held responsible for issuing fixes when it breaks?

A survey by ForeScout of 500 CIOs and IT decision makers found that 47% admitted to not updating default passwords on all IoT devices when they are added to corporate networks, and 15% admitted to not keeping security patches up-to-date.

Tom Salmon said that IoT is "one of those things that is known about and everyone knows it comes down to authentication" and while updates are done, IoT remains "a known quantity." He said that he could see the concern on how IoT uses "data appropriately" and how data can be managed and disposed of efficiently, pointing heavily to those who saw GDPR and data protection legislation as a key driver for cybersecurity.

Ultimately, this is a technology that is "a known quantity" as Salmon said, and something that has arrived at cybersecurity's door and has to be dealt with. Steve Durbin said that the all-pervasive nature of cyber will affect every aspect of what we do, from mobility through to smart cities and the inevitable impact of technology on our daily lives.

"The combination of all of these points of exposure will force a change both in our views on security and the way in which we handle and share information at the individual, corporate and inter- and intra-governmental levels."

Do IoT devices create an inherently wider attack surface? Scott Crawford answered that as computing becomes increasingly pervasive and 'smart' devices, endpoints and physical systems embrace IoT technologies that could

greatly expand those opportunities for the attacker.

It could be determined that IoT arrived a few years ago and the introduction of mobile device management technologies in the past 10 years could be enabled to work with IoT devices, but ultimately this is a sector will drive both innovation and attacks forward.

Conclusion: Is Cybersecurity in a Good State?

In order to draw a line under research like this, *Infosecurity* asked all respondents if they thought the cybersecurity industry was currently in a good place, and what its current strengths and weaknesses were. Of the professionals surveyed, 27 answered the question with the majority (20 people) undecided on a 'yes and no' perspective. Of the remaining seven, four gave a positive answer, and only three said that it was in a bad place.

Firstly, those who said 'no' gave a combination of reasons including professionals who "lack a true understanding of risk and as such do not make best use of their resources" and "who are struggling without sufficient resources to adequately address the proliferating array of risks confronting their businesses."

Also, a respondent said: "We persist in an environment where non-technical leaders are making decisions that directly impact technical work, and – more importantly – these decisions dramatically impact IT and information risk within an organization, which results in more negative risk and personnel frequently being put into lose-lose situations."

From those who said 'yes', there was a consensus that things are moving in the right direction, and that the industry is in a good state despite "what a complex mess technology is, and considering how much can be made from cybercrime.".

There was also a consensus that "security will continue to take a back seat" until there is a better understanding of technology and appreciation by the board. However, as one respondent pointed out, "people ask us questions that they were not interested in a few years ago and they are more aware and take it more seriously – and that is a good sign."

For those who said 'yes and no', there were various reasons given, such as: a lack of appreciation by the business, not sharing information or success stories, a lack of accountability, increased spending yet cybercrime increases, too much FUD-based selling, too much of an insular nature, the failure to overcome the skills gap and spending on technology which does not solve any problems.

Cybersecurity is a tough thing to measure in terms of its success – after all, money is paid and effort is made to defend, and you're only as strong as you can test and simulate. Despite that, this industry remains buoyant after a busy year of media coverage and the fast emergence of cybersecurity as a serious business risk END

Key Report Takeaways

GDPR is driving cybersecurity spending and behavior now, and will continue to do so in the next five years

Attacks are easy to carry out, can hit a multitude of targets and the defender must defend using the best resources they have

While the cloud is persistent and omnipresent, it requires skilled people who do not make common mistakes

AI and automation could be a driver for cybersecurity spending and behavior in the next five years but its benefits could be outweighed by the skills required to work with it, and an enhanced attack surface