STRATEGY / INSIGHT / TECHNOLOGY

infosecurity

State of Cybersecurity Report 2019

infosecurity

STATE OF CYBERSECURITY REPORT 2019

In 2018, *Infosecurity* undertook a research project to determine and explore the key trends that were driving the cybersecurity industry. Free from commercial influence and marketing incentive, this piece of research was intended to illustrate what a sample of security experts considered to be the factors driving the industry forward.

This project became the *State of Cybersecurity Report*, which proved to be very popular with our readers. A few months on, the decision was made to repeat the research and publish a report for 2019.

A chief aim of our research was to avoid an issue that seems to affect many published threat reports: research determined to drive the reader to a product or service. This year, we interviewed 60 industry professionals from across the globe, including investors, users, consultants, evangelists and business leaders, asking them what they felt were the key trends impacting the industry now and in the future. We then reviewed those responses and identified the common findings and now present them to you in this report.

We hope that you find this research interesting and that it serves as proof that as wide and varied as this industry is, in some ways, we think on a similar thread whilst some people can still highlight the anomaly.

Dan Raywood
Contributing Editor, *Infosecurity* Magazine

CONTENTS

TOP FIVE TRENDS

Trend 1: Better Defense and Products – 35% of Respondents

The trend that was cited most frequently by our respondents was the need for better technology, in terms of both the quality of detection and the convergence of technology itself.

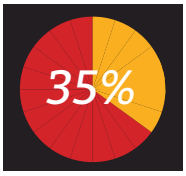
Many of the respondents that *Infosecurity* spoke to referred to the problem of consolidating technology. Simon Church, general manager and EVP Europe at Optiv, said that consolidation gets harder as the threat landscape gets bigger, causing users to "stop talking to vendors or go with one to reduce the noise level." Likewise, his colleague Andrzej Kawalec, CTO of cyber transformation and director of strategy and technology, advised that any new CISO in the first 90 days of a new job should not "buy any technology or products as they won't know what they need" in the early days of the role.

A number of respondents were clear on the issues of basics being skipped when it comes to the purchasing of technology. Nicola Whiting, CEO of Titania, said that a back-to-basics approach has come about because "people are realizing that the big-ticket solutions that they bought to solve a lot of their problems haven't delivered," something that Quentyn Taylor from Canon Europe agreed with. Taylor said that there is "no point in buying an expensive tool if you have to bolt it on the side."

Another factor surrounding technology problems is that of legacy technology. While the subject of the cloud had its own set of responses, the challenge of older products working with advancing technologies was also cited as a trend among our respondents.

Author and ISACA London Chapter director Raef Meeuwisse said that companies are often still running software and platforms that are out-of-date or full of vulnerabilities, while Pinsent Masons CISO Christian Toon said that "historic data and technology make it more difficult" to work with legacy systems and that there are "too many clichés of underinvestment and customization and scalable technology."

> ***"People are realizing that the big-ticket solutions that they bought to solve a lot of their problems haven't delivered"***



35% of respondents said better defense and products was a key cybersecurity driver

Marc Rogers, VP cybersecurity strategy at Okta, added that security is "sitting on a massive mountain of old technology." Whether it's applications written more than 15 years ago or protocols written 30 years ago, Rogers argued that we are too reliant on protocols such as SS7, "which has not evolved, as to change something so massive requires companies to change at the same time."

Despite these issued being raised, users were in agreement on the problem of complexity. Gil Shwed, CEO of Check Point, highlighted complexity as a key driver, specifically with there being as many as "16 attack vectors for just 26 technology sectors," an imbalance that will increase over time. To solve that problem, "you need to be super sophisticated and smarter than Einstein," Shwed said.

Nick Nagle from Condé Nast explained that he is seeing more convergence across the technology space thanks to the move from firewalls to unified threat management, and more established vendors offering "mobile, cloud and CASB (cloud access security broker)" technologies as they "look at the vertical stack."

One of the key elements regarding the technology problem was that of detection. Wade Baker, founder of the Cyentia Institute, said there's more data available from all of our security products, tools, practices and audits than ever before, while consultant Ted Demopolous pointed out that most vendors claim that they can do anomaly detection. "However, if we look back in perhaps five or 10 years' time, it will be apparent that we are now in the Dark Ages of anomaly detection and just starting to emerge."

Don't come away from this section of the report with the feeling that it is all bad, though. Javvad Malik, KnowBe4, said that "it is also important to talk about what we have achieved," as while it seems like things have got a lot worse, they have actually got a lot better.

He explained that in the early 2000s, buying, installing and managing a firewall was quite difficult, while security information and event management were "multiyear projects to deploy." However, now everything is much more standardized.

As we have covered, the problems surrounding technology encompass many factors, but there was notable positivity among the respondents' comments. Although legacy technology and a lack of interoperability can reveal the gaps in a company's network, we are seeing M&A activity and new vendors emerge, often backed or led by industry practitioners, to solve common problems.

Trend 2: The Human Factor – 31% of Respondents

According to 31% of respondents, the wide subject of the human factor in security was one of the main drivers in the industry. The reasons for this are broad: the human factor covers all elements of the apparent skills shortage, the need for better training and the 'human is the weakest link' consideration, as well as the concepts of awareness and simulation programs.

There was certainly a division in the responses we received regarding strategies for addressing and resolving the 'weakest link' of the human in security. Steven Furnell, associate dean of international and postgraduate and professor of IT security at the University of Plymouth, said that "it's a shame that we still hear the mantra that 'people are the weakest link' and yet still see so few attempts being made to support them."

There were various opinions about whether the human was in fact the weakest or strongest link within security, with differing perspectives about how things can be improved. On the side of training, Ed Tucker, co-founder of Human Firewall, argued that there needs to be an understanding that "everyone is a customer of security," as the user is the person who clicks on links. So if users are thought of as customers, it is "an opportunity to be better."

Fareedah Shaheed, CEO and founder of Sekuva, said that she sees more investment in "empathetic awareness" to better support people, rather than blaming them, which has been the case when humans have been held responsible for cases of data loss.

One strategy for improving the situation is better training. Jason Steer, director of EMEA pre-sales at Recorded Future, said that there is a need to get the resources to "upskill junior people" into senior security roles so that they can make better decisions "without having to have 10 years of experience." In the hiring process, there is often too much expectation that people will be ready to work at a high level and have a technically capable background, Steer added.

Sam Curry, CSO at Cybereason, agreed, saying that there is no talent deficit, and if there is then "we are creating it ourselves. If we thought differently about it, we could recruit [more workers], as there are tons of people who would like a job in cyber and we shouldn't make it more difficult for them to get one."

Despite industry statistics suggesting that things could be getting better with more initiatives intended to lure new people into jobs in the cyber industry, we are likely to be having these types of conversations for years to come.

Another aspect cited as impacting the human factor of security was the role of technology. Becky Pinkard, VP of IT and intelligence at Digital Shadows, said that she saw many companies at this year's RSA Conference with a message of "we can help you solve the human factor," so despite new "initiatives focused on training and user experience and awareness," there is clearly more work to do.

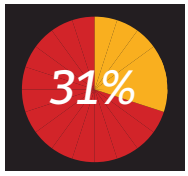
Likewise, Ron Gula, president and co-founder of Gula Tech Ventures, said there needs to be more adoption of technologies to aid people, but there is not enough focus on training.

If the technology to help address the issues exists, why is it not working? Tim Sadler from Tessian said that we built technology to stop spam arriving in our inboxes, and now we "need to ask more from technology and limit human risk." However, the problem is that it is not user friendly and we're not providing a more seamless experience for users, Sadler argued.

Is this where there is a collision between the human factor and the technology to aid it? Martin King, CTO of the Football Pools, felt that it "doesn't matter how many technical controls security and infrastructure teams put in place, the simplest and often quickest path to a breach is through social engineering. We can put the most sophisticated technology in the world in place, but if a user gets a phone call from tech support asking them for their password and they oblige, it's game over."

It appears that even though the human factor of security is a major trend, solving it is not an easy task. Rob Clyde from ISACA noted that until organizations are better equipped to deal with the challenging threat landscape, including making appropriate investments in their workforce and continuous training, the volume and impact of cyber-attacks will continue to escalate.

> ***"We have seen some organizations 'shelve' or alter cybersecurity projects to focus on projects that are driven by the regulatory landscape"***



31% of respondents said the human factor was a key cybersecurity driver

Perhaps things are moving in the right direction, though. Dr Jessica Barker, co-founder of Cygenta, said that there "has been a huge increase in understanding, over the last couple of years alone, in the importance of the human side of cybersecurity" and the need to take a holistic approach.

Dr Barker added that there has been a "greater emphasis put on awareness, behavior and culture in cybersecurity." That is a welcome change, she added, as we're no longer having to explain what cybersecurity is and organizations are spending time and money on assessing and addressing their culture.

Trend 3: Compliance – 25% of Respondents

Compliance was the standout industry trend in our 2018 report, most likely because we were in the lead up to the deadline for compliance with the General Data Protection Regulation (GDPR). In the following year, the subject of compliance has remained a significant talking point with the introduction of the Network and Informative Security Directive and the California Consumer Privacy Act (CCPA).

Analyst Bob Tarzey said that while "excitement about regulation has died down a little," regulatory controls will remain a driver in the EU and beyond, while Dr Barker said that "more and more organizations are changing the way they handle data" in the face of changing regulatory requirements.

She added: "This obviously drives cybersecurity in some ways, but we have seen some organizations 'shelve' or alter cybersecurity projects (awareness campaigns, for example) to

focus on projects that are driven by the regulatory landscape."

So has GDPR partly been a hindrance to cybersecurity, effectively preventing the advancement of certain projects because of fear of regulatory fines, or has it provided data protection?

Izzy Vixsama from Vix Cyber said that the "anticipation and stress of implementing GDPR and privacy" was a problem for businesses in her native USA, as despite the May 2018 deadline, a lot of companies today are still not fully aware of what GDPR is and do not have a strategy for it.

"Some companies are not trying to understand what it means for their organization and that is going to cause a shift in how data is collected here," she said.

Assessing further feedback and comments, there does appear to be a feeling that the introduction of GDPR has had both positive and negative impacts on the security industry. Ted Demopoulos pointed out that while being compliant and being secure are very different things, compliance is a step in the right direction. Also while some laws, although well-intentioned, may be overreaching to the point of absurdity in their current iteration, he expected them to "improve substantially over time" and thought the "overall effects are extremely positive."

However, from a more negative standpoint, respondents noted concerns around the prospect of large monetary penalties or conversely failures of data protection regulators to actually push the regulatory charges. Martin King said that, after the initial scare, GDPR hasn't led to the monetary fines the world expected.

He theorized that this would lead to most businesses withdrawing, or scaling back, the longer-term funding plans they had in place to support the change.

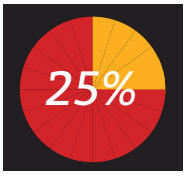
Likewise, Chris Hodson, CISO of Tanium, stated that what hasn't helped is a lack of very high-profile "slaps on the wrist." He referred to the Google fine in France but suggested that "it was a manageable figure."

However, GDPR and other compliance regulations have done a lot to promote the cause for effective incident response. Security consultant Neira Jones said that new compliance frameworks had "forced better incident response practices, and all those in the cybersecurity field are rubbing their hands together."

Aside from GDPR, there are other compliance frameworks that drive cybersecurity forward, including the Second Payment Services Directive (PSD2), which also introduces incident response requirements.

CCPA was noted as a particularly outstanding example of a new act bringing about regulatory change in the USA. Rob Clyde, chair of the board of directors at ISACA, said that there is an increased emphasis on landmark privacy regulations and that these "will put an added emphasis on the connections between cybersecurity and data privacy, and the need for a holistic approach to dealing with these challenges."

Matt Pascucci, cybersecurity practice manager at CCSI, said that CCPA "is trying to throw a wider net over things," a result of GDPR stipulating that a privacy officer must be put in place, something that will be taken seriously in the USA.



25% of respondents said compliance was a key cybersecurity driver

Compliance is a complicated trend to fully evaluate, because while it is something that needs to be acted upon, as Hodson and King said, the stronger enforcement and regulatory fines that had been hyped up in the build up to GDPR have not really materialized. Therefore, it may force some to think that compliance does not have to be taken as seriously as we are expected to believe. Nonetheless, with GDPR and CCPA cited frequently by our respondents, it is clear that regulation remains a key element of the cybersecurity industry.

Trend 4: The Company and Board Engaging with the Security Team – 18% of Respondents

According to 18% of our surveyed demographic, another driver impacting cybersecurity was businesses' engagement with security teams and vice versa. The issues here are very clear: if the security team understands what the business is trying to achieve, then it has a better chance of succeeding. If the business understands who the security team is and its policies and challenges, then there is a better chance of a more secure culture.

Thom Langford from (TL)2 Security said that it is not the job of security to make the company more secure; "it is to help it sell stuff and help it meet the vision and the goals that the business has set itself." Langford claimed that one of the problems is that people will not actually read the company report, and if they do not, how do they "know what the company is trying to do and how it is trying to achieve its goals?"

Amit Yoran, CEO of Tenable, said that "you're seeing audit and risk teams report to the board of directors on a regular basis." He agreed with Langford that two things move corporations forward – making money and the fear of being caught doing something that will embarrass the brand – and security can help reduce the latter problem.

ISACA's Clyde said that he thought that boards of directors have been far more active and interested in cybersecurity in the last couple of years, which he called "important progress," as successful organizations regularly have cybersecurity on the agenda at board meetings. Likewise, Cyentia's Dr Barker said that there is an increase in board awareness and global regulations, which are "converging to raise accountability for cybersecurity programs."

Moss Adams CISO Nathan Wenzler thought that there had been a realization that "culture and soft skills and human stuff [are] incredibly critical and important," because people working in cybersecurity are not pure technologists. Security teams know that it is "time to take action themselves." He claimed that people "want more power and more control," but security should be about helping businesses communicate with each other.

It's not just about "being at the table," he said. "We have to take charge to be responsible for culture and educate better and find ways to explain a complicated problem in an easy way."

This level of understanding that cybersecurity is a problematic issue seems to be consistent, but is it easy to overcome the problem to find the solution? Joseph Carson from Thycotic argued that the job of the cybersecurity professional is not to find the solution, because if we spend all of our time doing that "we will never solve cybersecurity."

He said that the job should instead be seen as a business risk, and professionals need to align themselves to the success of the business. "Our job is to help people be successful and help executives do their job – do business first and we should be changing everything we do to a business risk with people and technology being part of this solution, process, standards…everything."

The notion that it falls upon the professional to drive the agenda may not be so appealing to everyone. It requires the user to be the driver of the relationship, and if they are met with any form of resistance or even a degree of disinterest, any culture or convergence changes may not last long.

Meeuwisse said that overall it does not appear that the C-suite has come to grips with existing issues, while Professor Alan Woodward argued that the "boardroom is where lessons are not learned," as there are too many issues that are not understood or learned from.

Meanwhile, Ed Tucker said that there is still a "weird view of security as an ivory tower," and Steven Furnell pointed out that while cybersecurity "is undoubtedly taken more seriously by today's organizations than it was in the past," if you took away drivers like GDPR, the default cybersecurity attitudes and behaviors possibly haven't changed.

Furnell asked: "Have the lessons really been learned or are we faking it? Would organizations go back to ignoring it if they thought they could get away with it? A true culture of cybersecurity still seems some way off."

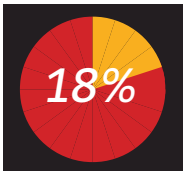
> ***"A true culture of cybersecurity still seems some way off"***

Achieving a true culture of security is not without its challenges. As it seems from these comments, if the board is as engaged as the security team, there can be a winning mentality, but if there is disinterest on either side, a true culture of security will not emerge. Business engagement is a clear driver for cybersecurity as it can mean improved culture, leading to better adoption and budget…if things are done well.

Trend 5: Automation and Machine Learning – 18% of Respondents

While machine learning is often maligned for being a marketing term used by vendors to better boost ageing detection technologies or even as an extension of monitoring technology, it's hard to ignore the overarching trend of automation, which was cited by 18% of respondents.

Respondents relayed concerns about the reliability and hype surrounding autonomous tech, yet the overall feedback was generally positive. Recorded Future's Steer noted that a lot of companies are "riding on the bandwagon," as different vendors say different things regarding the effectiveness of AI or machine learning. Meanwhile, Tucker said that though there are concerns about a lack of understanding regarding different types of AI, there will come a time when we will have to "put faith in the accuracy" of machine learning.



18% of respondents said security C-level and security team engagement was a key cybersecurity driver

Ross Brewer, vice-president and managing director EMEA at LogRhythm, said that there is a lot of hype suggesting that "machine learning is the greatest thing since sliced bread." While machine learning and unsupervised learning are excellent at detecting anomalies, there is too much belief that anomalies are always bad, he said, when actually "they just show what is abnormal or different."

These comments suggest that machine learning and automation are negatives, and you may wonder why something that is so frowned upon should be a cybersecurity driver. Like many aspects of technology, there are both proponents and opposition.

According to many of those we surveyed, AI and machine learning were drivers of the future. For example, Ben Tomhave, Falcon's View Consulting, said that the "imperative for infosec must be automation first and humans second" as too many SOC templates are old and broken. "All of these things need to be rethought and rebuilt from the ground up, and this can't happen soon enough," he said.

Tomhave also stated that endpoint protection could do with a heavy dose of automation, as there is a lot of opportunity to build an optimized security stack on endpoints that give us a lot of capabilities "but that are all built around automated orchestration and configuration management above all else."

Okta's Rogers explained that AI "offers immense value and fear" as it is not that sophisticated yet, but can aid humans in doing certain things "and adds scalability and dynamic scalability and the potential to offload 60%–70% of routine analysis tasks."

For Pinsent Mason's Toon, machine learning and AI, as well as data aggregation and the "ability to interrogate to aid in detecting and the alerting of networks," will broaden the view from a simple log and will allow aggregation from data feeds from management systems.

As mentioned earlier, there are positives and negatives to the automation trend, but the benefits of automated systems cannot be ignored. The realities of the number of alerts and the time required for a human to investigate those alerts have led to this technology being adopted and, hence, the skepticism surrounding it has emerged. Whether this is truly a positive or negative topic depends on your perception and experience, but automation and machine learning completed the top five industry drivers noted by our research respondents.

REMAINING TRENDS

Along with the top five trends we have already explored, there were 26 other drivers cited by our respondents. Some of the single-mention trends you'll read about in our following section, but some only just missed out on being listed in our top five, so they deserve their own mention.

Business Agility and Digital Transformation – 13% of Respondents

The move to a more agile business model has been on the lips of business leaders recently, and as a result, security is left to catch up. However, this involves the concept of shifting left and DevOps, often with security included as part of that. Security researcher Adrian Sanabria said that as businesses "step into agile and the automated space, security can be impossible at that scale," and as services are not given proper attention, companies can "end up like another Equifax."

Ed Tucker added that in some companies, security already sits in digital transformation, while others are just starting the journey "and security needs to find a place in there."

One company that has built its offering around the digital transformation shift is Signal Sciences, and co-founder Zane Lackey said that this trend "is upending security and the way it has been done for 20 years." For too long, security acted as a blocker and a gatekeeper, and the journey to the cloud and DevOps were about bringing siloed capabilities together.

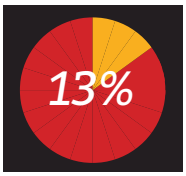
This is a major driver, as Lackey said that security is meeting an environment where apps, once changed every 18 months, are now changed 100 times a day. "If security wants to stick its head in the sand, the business is just going to move forward without them, and it is a powerful opportunity if embraced correctly."

Cyber-Hygiene – 15% of Respondents

The concept of getting the basics right has been present for years, as the majority of data breaches are a result of bad cyber-hygiene, as incidents like WannaCry proved in 2017.

Titania's Whiting pointed out that "fundamental, basic security practices are still not being applied consistently and at scale."

Thales cybersecurity evangelist Jason Hart also said that he was "amazed by the number of organizations not doing the basics," despite more money being spent and larger breaches than ever before.



13% of respondents said business agility and digital transformation were key cybersecurity drivers

> ***"Fundamental, basic security practices are still not being applied consistently and at scale"***

Some common concerns involved the problems of password security and reuse, as well as what fitted into our previous section exploring the human factor of security. If the basics do not include what your employees are doing and what they are made aware of, who is expected to take the blame for that?

The Cloud – 13% of Respondents

The proliferation of the cloud is a topic that has already been referenced several times within preceding sections of this report as part of larger business trends. However, as Ben Tomhave explained, as security and risk professionals, "we should embrace multi-cloud as a smart risk decision, but at the same time, we need to make sure smart decisions are made within each cloud provider's environment, too."

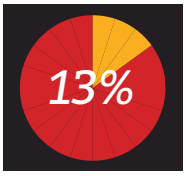
APT and Nation State Attacks – 13% of Respondents

Sometimes dismissed for being too much of a marketing term and summarizing the FUD factor, advanced persistent threat (APT) still scored highly among our respondents, along with state-sponsored hacking. Perry Carpenter, strategy officer at KnowBe4, said that more politically charged attacks are pushing security forward, particularly with (often automated) social media posts that publicize inflammatory messages and human-generated actions where a phishing e-mail can appear to come from a country that attackers want to pin blame upon.

Becky Pinkard of Digital Shadows said that APT is being discussed more commonly, regardless of whether it is legitimate or not. However, the problem here is that many victims of APT attacks are not sharing details on them, "and this is leading to less understanding."

Consultant and speaker Graham Cluley said that nation state attacks were, for him, the key trend at the moment, as many companies feel that the attacks do not affect them, but they may have "customers who are of interest to a nation state."

Echoing Pinkard's comments, Cluley said that cybercrime has "grown up," as has the cybersecurity industry, but too much childish behavior and a failure to work together because of rivalries means that too much time is spent putting out fires, and we do not share information on "organized businesses."



13% of respondents said APT and nation state attacks were key cybersecurity drivers

> ***"The bad guys are ahead and will be for the foreseeable future"***

Tomhave continued, saying that as has been the case since the cloud took off, we will see an emphasis on host-based tooling over network tooling, "if only to minimize complexity and maximize consistency."

Scott Gordon from Pulse Secure highlighted "the means to apply granular, segregated access to applications and resources in the data center and multi-cloud" as one of four trends driving the incorporation of zero trust architectures, while Aurobindo Sundaram, head of information assurance and data protection at RELX, said that cloud adoption is resulting in automatic segmentation of assets.

Quentyn Taylor thought that cyber wars have escalated to "states attacking each other," something that is now being done openly. Taylor called Stuxnet a watershed moment, as now we see attacks like WannaCry and Destroyer and state-sponsored attacks on the front pages. "Your investment plan may hinge upon who is in charge politically," he pointed out, and this may now impact you.

Malware, Attacker Sophistication and Ransomware – 13% of Respondents

The final remaining trend was also about attacks, but rather than being specific to nation states it was more about malware and the attackers behind it. Bob Tarzey called this "the greatest concern expressed by security managers" as attempts to gain access to networks continues to drive security and "keeping these threats at bay is a big driver."

Laurence Pitt, cybersecurity marketing and strategy director at Juniper Networks, said that there is a trend of "more basic attacks coming through." While attacks will migrate from using botnets to using AI techniques, the number of exposed databases enabling phishing attacks will increase.

In last year's report, the expanding threat landscape and evolving attacks accounted for 34% of responses, with the major ransomware campaigns of 2017 being a likely reason. Despite being predicted to be on the downturn, ransomware attacks were driving cybersecurity, according to Izzy Vixsama. In particular, there were more attacks on senior citizens as they tend to have more money and on younger individuals who have good or no credit history, as they can be targeted in fraud attacks.

Nathan Wenzler too thinks ransomware is still the main malware driver, as people are still not reporting it and companies are still failing to have adequate backup strategies, so when they are hit they "don't know what to do."

As for the state of attackers, there was agreement that "the bad guys are ahead and will be for the foreseeable future," as Martin King said, stating that attackers are using automated and cloud services, giving them "plentiful resources which are easy to play with."

Martin Lee, manager of Talos Outreach EMEA & Asia at Cisco, said that it was "still a matter of bad guys looking for systems to offer them the most opportunities for the least effort and least risk," and known vulnerabilities reduce the need for zero-days. Lee did highlight increased attacks on routers and DNS servers but said that malware very much follows an evolve-and-cycle movement. Fixing this problem falls to the basics of patching systems and having visibility of systems and network traffic.

SINGLE-MENTION TRENDS

While the top trends were determined by the responses we gathered this year, it was also interesting to see several drivers that were cited by only one person. Rather than disregard these, we list them here:

- Governance, risk and compliance tools
- Certificate transparency
- Managed services
- Financial motivation of attackers
- Ratings and metrics
- Fraud
- Bug bounties
- Government factors
- Fuzzing

You may look at this list and think that some of the things noted deserve to have been cited by more people, and there may even be some things you might not have heard of.

It was particularly interesting to see bug bounties cited only once, with respondents saying that these can be used effectively to test the underlying security of a platform and, when combined with a permissive vulnerability disclosure policy, can make the entire industry safer.

It was somewhat surprising that fraud, financial motivation and government factors (which encompassed policies and standards, common definitions on what is acceptable and how much government understands cybersecurity issues) were not cited more than once. As for the more technical concepts of fuzzing and certificate transparency, perhaps it is not surprising that these were cited only once. Maybe in a future report, we will see these trends become more popular.

FUTURE TRENDS

As well as what is driving cybersecurity right now, we also asked a portion of our respondents what they thought would drive the industry forward in the next five years. A sample set of 33 responders delivered 16 distinct trends, with one far ahead of the others.

Advanced Automation

Automation was the standout trend for the future, with 36% of respondents citing it.

Kerry Bailey, CEO of eSentire, said that machine learning capabilities will "help analysts do deep analysis" and be more alert on what to look for, "including indicators of compromise that don't fit patterns but still require investigation." Bailey also said that we've reached a point where we cannot rely on people alone, and new methods of investigation are needed.

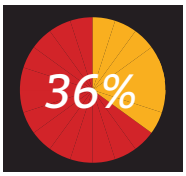
Rajan Kapoor, director of security at Dropbox, added that machine learning "can finally solve the last-mile problem of data-loss prevention and rights management" because, as long as employees make a call on the sensitivity of the data they are working with, the margin for error is too large.

Kapoor also said: "Machine learning has the potential to hide the messiness of classifying data from employees while applying the right data classification, protections and rights management behind the scenes. It will be a win for companies trying to keep their sensitive data secure and will be a win for employees who just want to get work done."

Across the responses, though, AI featured very prominently. Nick Nagle said that automation is "huge" and that we're currently only scratching the surface of its possibilities. Likewise, Nicola Whiting said that machine learning and AI "are not going away as [they're] the only viable choice for defense at scale," but time does need to be taken to allow it to mature and become more consistent in its delivery.

"One of the key changes needed to deliver viable, AI-driven autonomous mitigation and defense will be the movement away from legacy technologies which create probabilistic data (such as scanners) towards those sources that create deterministic data (e.g., event data and configuration analysis)," Whiting said. "This will be an essential requirement as any AI empowered to make defensive decisions will be extremely reliant on data accuracy."

However, the notion that there needs to be more patience with AI's capabilities and an avoidance of complete reliance on it was common, as Sundaram said. While advances in orchestration and automation will narrow the gap between breach and detection for incidents where rule-based detection is possible, "the lack of effective detection rulesets and smarter attackers will continue to post challenges to organizations," he added.



36% of respondents said advanced automation will be a key driver of cybersecurity in the future

Elsewhere, the responses very much followed our current trends, with board interaction, attacker mentality and the human factor all proving popular. There were a total of six single-mention trends, too:

- Encryption
- Containerization
- Visibility
- Nation state level attacks
- Steganography
- Blockchain

Conclusion

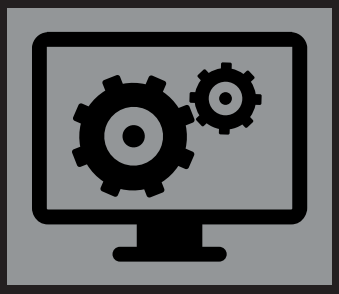
To draw a conclusion about this variety of perspectives is rather challenging, as respondents to our research cited so many trends driving cybersecurity forward. However, a standout takeaway is that, whether caused by cloud, digital transformation or attacks, businesses and security teams are changing. This is clearly not a static time in cybersecurity.

As we have discussed in this report, it is not the job of the security team to lock down a business. Instead, its job is to help the business operate and meet its vision and goals. If the business wants to change, then security needs to be there to enable that change and not stifle innovation.

The biggest change evident in our research this year is the drop of compliance from the main driver in 2018 to the third driver in 2019, leapfrogged by both the human factor and technology issues.

Compliance dropping to third place does not suggest that it is any less important, and its top placing last year may have been down to the GDPR compliance deadline. The day-to-day work of the security team seems to be the top driver this year, and as we move forward the human may be replaced by automation, and trends will change again END

Key Report Takeaways

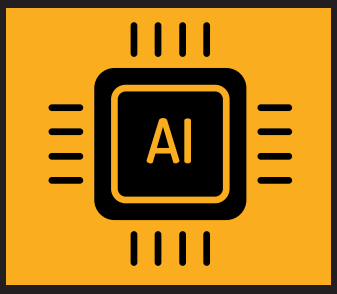


Tech Troubles

Technology was cited as the top cybersecurity problem by our respondents, highlighting issues such as cohesion struggles, purchasing confusion and an over-saturated tech market

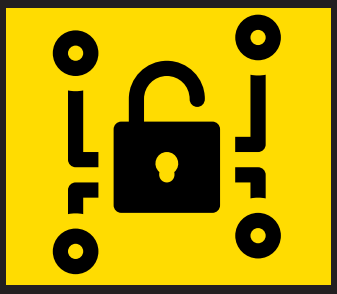
Compliance Complexity

A year after the GDPR came into force, the topic of compliance remains a top trend and driver within the cybersecurity industry



Automation: Believe the Hype

Despite machine learning and AI often being described as 'hype,' our research found automation to be among the top trends now, and the most cited trend for the future



Sophisticated Attacks, Sophisticated Attackers

The standard level of attacks remains high and sophisticated attackers pose a significant challenge for security to battle with