STRATEGY / INSIGHT / TECHNOLOGY

info security

State Of Cybersecurity Report 2020

infosecurity

STATE OF CYBERSECURITY REPORT 2020

Welcome to the third annual *Infosecurity* Magazine *State of Cybersecurity Report*. *Infosecurity's* first iteration of this research report was launched back in 2018, featuring the results of a survey of 32 security industry professionals outlining the key trends impacting the sector at the time. A year later, the second instalment of the report collated insights from a larger cohort of 60 expert respondents, again depicting the most important themes affecting cybersecurity. Highlights and findings from both reports have since been presented at various events and conferences – both physical and virtual – over the past two years.

As *Infosecurity* prepared to bring together this year's report, it was clear that a new research angle would be required to inject fresh insight and learning outcomes to the data gathered, along with continuing to deliver the same overarching industry analysis.

Therefore, the findings of this year's report are based on feedback from 75 security professionals representing three distinct verticals; 25 from academia, 25 in the investor space and 25 either advising on security or implementing, using and selling solutions. This has allowed us to not only present and outline the most influential security trends affecting the industry as a whole, but also reflect upon and compare the trends most influential within different sectors.

As you will read, a new, major trend has dominated this year's research, whilst topics that proved popular in past reports have remained present.

The *Infosecurity* team has enjoyed conducting and bringing together this unique piece of research. I hope you enjoy reading this year's report.

Dan Raywood
Deputy Editor, *Infosecurity* Magazine

CONTENTS

TOP FIVE TRENDS

TREND ONE:
The Impact of COVID-19
– 30% of Respondents

As was the case in *Infosecurity's* first *State of Cybersecurity Report* back in 2018, a central 'black swan' event has dominated our research findings this year. Two years ago, it was GDPR compliance that stood out as the key trend impacting the information security industry at the time. This year's research has discovered a new most influential trend cited by 30% of respondents... the information security implications of the COVID-19 pandemic.

The impact of the pandemic on cybersecurity has been vast, bringing with it waves of change in the way we work and secure our workforces. Ajay Arora, founder and CEO of BluBracket, said "the spread of COVID-19 completely changed the cybersecurity landscape" as "companies strained to quickly enable remote working securely." He also said that this has meant that many long-term projects have been put on hold, as resources are scrambled to equip remote work, something he expects will "dominate all cybersecurity efforts for the next three months" with greater emphasis placed on remote working strategies for the long-term.

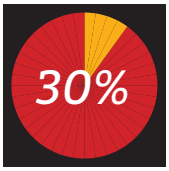
> ***"The spread of COVID-19 completely changed the cybersecurity landscape"***

Tech innovator and entrepreneur Dmitriy Akulov explained that even before COVID-19, more and more companies were becoming more dependent on remote work, but the pandemic accelerated that. "I believe that the pandemic will have lasting results on the workplace with more and more businesses – who were (at first) slow to the race – allowing workers to stay remote – at least partially," he continued.

Digital transformation has proven highly important during the crisis, according to Stephen Boyer, CTO of BitSight. "Our dependency on digital systems is only going to increase," he argued. However, when digital transformation investment is made too hastily, it can "leave doors open and creates a massive attack surface," he warned.

Rose Ross, founder of the Tech Trailblazers, concurred: "The proliferation of remote working has brought with it some new security challenges. For example, how do you manage an environment when you aren't physically in the office yourself? What is the best way to manage a team remotely? What has happened to the edge of your network?"

Another disturbing element of the pandemic cited was the growth of COVID-19-related attacks and scams. Arno Robbertse, chief executive of ITC Secure, said that over the last few months, cyber-attacks against the healthcare industry have risen by 150% as cyber-criminals have exploited the pandemic through various attack vectors. These variants include phishing emails pretending to be from the World Health Organization and more sophisticated forms of intrusion via encryption methods.



30% of respondents said COVID-19 is a major trend impacting information security

There is also the danger of remote workers being left more susceptible to attacks and scams due to poor vulnerability management strategies. George Krautzel, managing partner at MissionOG, said that there is a need for businesses to combine real-time vulnerability management of "disparate devices" to allow secure access to legitimate users, while negating unauthorized access attempts from bad actors.

Another harmful side effect of the crisis cited by respondents was the use of disinformation surrounding COVID-19. Safeguard Cyber CTO and president, Otavio Freire, said that disinformation about the pandemic has been widely used to target corporations and consumers with ransomware and spear-phishing.

As has been made evident thus far, the various security risks and challenges surrounding the COVID-19 pandemic were well discussed and outlined by respondents. However, some of those polled also cited the potential positives to come out of the unprecedented circumstances organizations have been thrust into.

Heath Renfrow, CISO and director at the Crypsis Group, predicted that companies will now adopt trends to better enhance the capability for workforces to work remotely and believes greater focus will be put on implementing stronger security protocols to reduce cyber-risks as a whole.

What's more, Rose Ross said that venture capitalists (VCs) are working closely with their portfolio companies to respond to the crisis, and C5 Capital created the C5 Cyber Health Alliance to better secure European healthcare organizations during the pandemic. This collaborative initiative provides the necessary support and means for hospitals and clinics to protect their internal systems and defend against unwanted cyber-threats. It will also provide additional safeguarding for work that pharmaceutical research and development facilities are doing while developing a vaccine for the virus.

It comes as no great surprise to discover that the impact of COVID-19 on information security was the most commonly-cited trend among respondents. For cybersecurity, COVID-19 has brought significant challenges – mass remote working, surges in attacks and shifts in networking – as well as provided potential opportunities for the industry to come out of the crisis stronger and be better equipped. However, the extent to which COVID-19 will continue to be a major trend for the rest of the year is unknown and the very long-term impacts remain to be seen.

TREND TWO: The Cloud

– 26% of Respondents

The wide-ranging subject of the evolution and development of the cloud was the next most common trend to be cited by respondents. Saj Huq, program director at LORCA, explained that organizations have greatly accelerated cloud usage as part of digital transformation journeys, and with this has come cost benefits and the ability to "enable more distributed workforces." However, Huq was also quick to point out that cloud proliferation has also led to various new and increased risk factors. Huq said there is therefore a clear need "to focus on solutions that secure the cloud."

Nik Whitfield, CEO of Panaseer, explained that very few modern businesses "are not working in the cloud" and he has seen notable increased usage of cloud Platform-as-a-Service (PaaS) offerings.

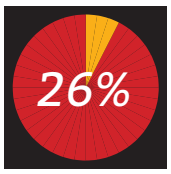
Likewise, Rafe Pilling, senior security researcher at Secureworks, pointed to growing numbers of organizations moving to cloud-based delivery methods as they increase their remote working needs – Microsoft Office 365 being a prime example. "More and more [businesses] accept that identity has therefore become front and center as a concept," and with the growth of the cloud, the traditional perimeter has eroded, he added.

Drilling down into the specific security challenges impacting cloud usage, Giovanni Vigna, director of the Center for Cybersecurity and professor at the University of California, Santa Barbara, said: "The cloud is moving at such a fast pace that we have not yet developed the modelling and analysis approaches necessary to understand the security implications of cloud-based deployments." He also highlighted the risks surrounding access of data via non-traditional devices enabled by distributed, cloud-based infrastructures.

Furthermore, Magda Chelly, managing director of Responsible Cyber, warned businesses against "over-trusting cloud services." An assumption that security is enabled by default is a common mistake made across industries and companies.

Likewise, Doug Dooley, COO of Data Theorem, advised companies to strongly consider how often they migrate their customer relationship management software into the cloud. He also said that companies must have a clear understanding of how cloud-dependent and widely distributed their cloud apps and environments are – something some businesses struggle with because "they don't have a full assessment of all of their cloud architectures."

> ***"We have not yet developed the modelling and analysis approaches necessary to understand the security implications of cloud-based deployments"***



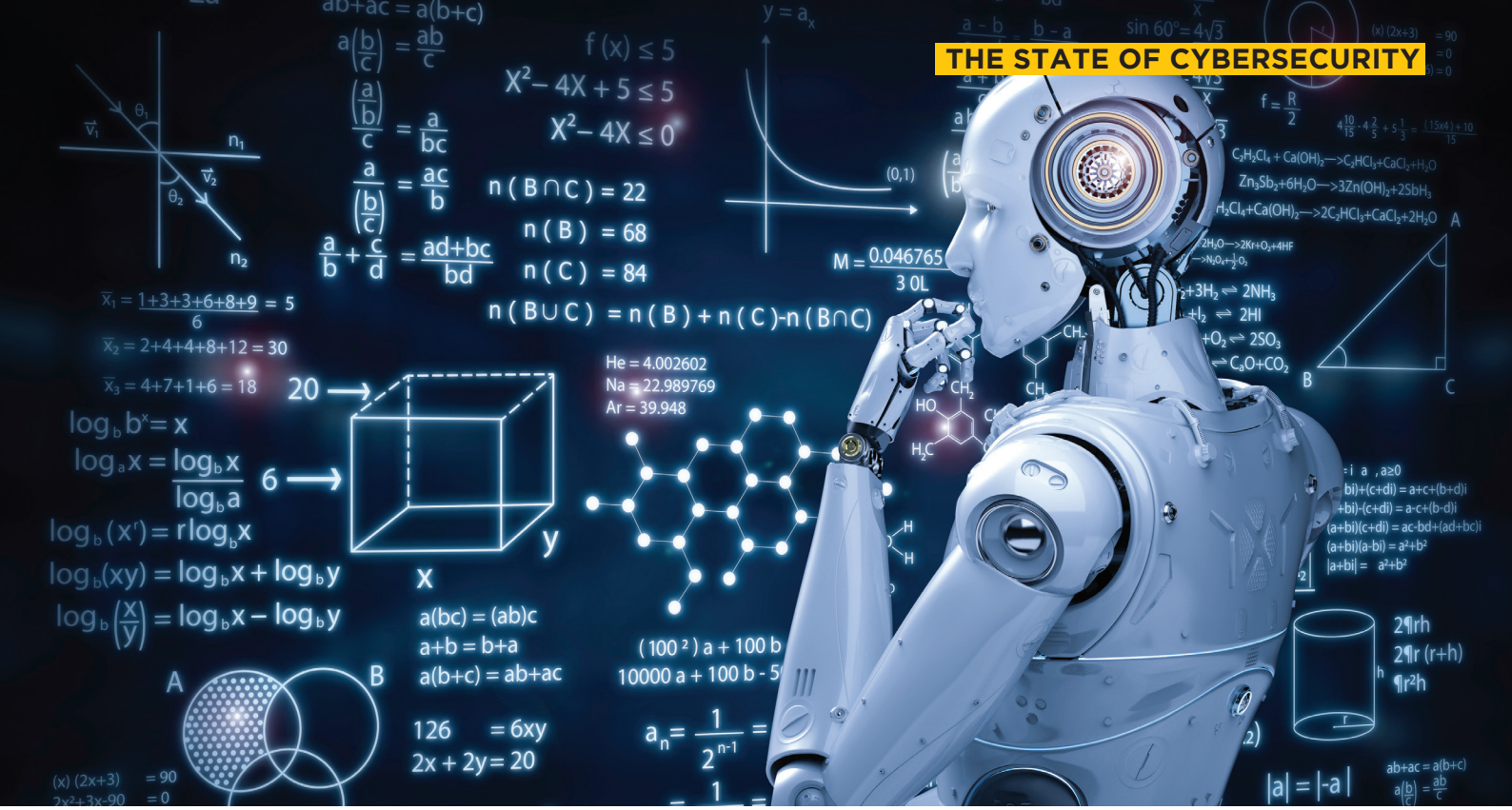
The cloud was cited as an important security trend by 26% of respondents

In contrast, George Krautzel commented on the business benefits of using cloud technologies. For example, he said, prior to the cloud, "innovation would routinely be stunted due to long wait times and delayed approvals of new hardware and software." However, the growth in cloud usage has meant processes are moving faster.

On a similarly positive note, Professor Keith Martin of the information security group at Royal Holloway, University of London, said he has been impressed by the Estonian government "essentially placing their entire data records into their own private cloud, as once an entire nation is in the cloud, the sky's the limit (excuse the pun)."

In fact, Olav Ostin, managing partner at investment company TempoCap, said that if a company does not have a cloud offering, TempoCap will not invest in it, so there are clear potential growth and development benefits to implementing cloud technologies for organizations too.

Cloud remains an important topic in security. For some, it is the way forward for enabling better business operation and agility, while for others, it is a constant data security and privacy risk. Either way, it continues to be a key factor in information security, and had the COVID-19 pandemic not impacted the industry so heavily this year, cloud could easily have been top of the list of trends impacting the sector.



TREND THREE:
Artificial Intelligence and Machine Learning
– 25% of Respondents

As was the case in *Infosecurity's* 2018 and 2019 industry reports, the impact of Artificial Intelligence (AI) and Machine Learning (ML) on information security was among the five most influential trends this year, cited by 25% of respondents.

Ayman El Hajjar, lecturer in computer science and engineering at the University of Westminster, said that AI and ML "still take up a large chunk of research and drive innovation in the industry."

The main use of these concepts is to enhance workforce development practices through the integration of tools, as well as augmenting workforce capacity through advanced automation and analysis, according to Diana Burley, professor at The George Washington University. "As the use of AI to develop autonomous and semi-autonomous systems grows, so too must the understanding of the human-AI interface," she said.

"Otherwise, the humans in the loop could reduce any gains in system security," she argued. "As such, the human factor as a component of linking AI and cybersecurity will grow in importance."

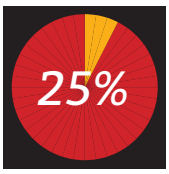
This relates to how AI and ML are used in modern workplaces, and investor and board advisor David Billeter believes that more focus will be put on "end-to-end" security automation, where changes on host and network devices are automatically made to respond to security threats. Likewise, Deborah Golden, risk services leader at Deloitte US, said she has seen a "huge pick up" of ML being used in threat intelligence to digest information. Furthermore, Imran Ghory, partner at Blossom Capital, said that with security teams often overworked and with too many duties, the addition of these technologies is adding "huge value" by freeing up security professionals' time.

Professor Keith Martin also pointed out that, whilst neither AI or ML are new concepts, "we now have the computing power to really utilize them," adding that the "smarter use of large data sets" is going to be a significant trend for some time to come.

> ***"We will continue to see evolution in the complexity of attacks as we evolve our own autonomous defenses"***

Another positive impact of AI and ML cited by respondents was in regards to orchestration. CISO and adjunct professor, Todd Fitzgerald, said it has become the norm for companies to automate "routine, time-consuming tasks" through AI and ML.

Vern Paxson, professor of computer science at the University of California, Berkeley, added that ML "can work excellently within domains and is great at coming up with powerful qualifiers around spam."



AI and machine learning are key drivers of cybersecurity, according to 25% of respondents

Then there's the advantages of using AI and ML to support intrusion detection systems, said Raj Muttukrishnan. He explained that there have been effective efforts made to increase the accuracy of intrusion detection systems by integrating augmented reality "so that the security analyst is given a 360-degree view of the network to make informed decisions."

There was also notable mention among respondents of the human element and its relationship with evolving AI and ML technology. Marcel Van Der Heijden, partner at Speedinvest, highlighted the issue of security teams struggling with huge numbers of security tasks and data sets. This is where AI and ML can step in, he claimed, aiding in code review and data sharing with "new machine methods and applications able to do so in a secure and compliant way."

However, not all responses regarding AI and ML were entirely positive from a defense perspective. Leigh Metcalf from Carnegie Mellon University's CERT (Cybersecurity) Division pointed out that AI and ML can work well "when used correctly," but warned there is more and more adversarial machine learning being used in attacks. "We will continue to see evolution in the complexity of attacks as we evolve our own autonomous defenses," she said.

Paul Ayers, executive in residence at Ten Eleven Ventures, agreed, noting that attackers are indeed leveraging automation and AI to wage wider attacks, therefore using the same technology to fight adversaries is more critical now than ever before.

As has been made clear in this section, the majority of responses relating to the use of AI and ML in cybersecurity were noticeably positive, with a few caveats and words of warning about the technology thrown in along the way.

TREND FOUR:
The Human Element
– 24% of Respondents

The ever-present debate topic of the human element of information security was the fourth most popular trend among this year's respondents, cited by 24% of those surveyed.

Professor Steven Furnell from the University of Plymouth cited three reasons why he believes the human factor is an important trend in the industry. First is the increasing recognition of the profession of cybersecurity: "This is positive for the profession and practitioners within it, as well as for organizations that want to be able to draw upon a professional community in order to address their cybersecurity needs."

The second reason involves the ongoing shortage of cybersecurity skills. "When looking at cyber-skills, we still face the fundamental challenge that businesses need to know what skills they need, and they need to know how to recognize them," continued Furnell, "and that's before the challenge of finding and paying for it."

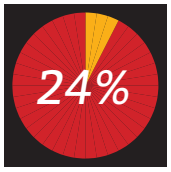
Third is the issue of a lack of basic cybersecurity literacy. Furnell said that this continues to contribute significantly to the breaches that we see, with people making poor choices, falling victim to scams and introducing vulnerabilities simply because they do not know any better.

For Sean Martin, adjunct professor at Pepperdine Graziadio School of Business and Management, another important factor impacting the human element of security is the need to better engage with educational content, as future cybersecurity professionals "aren't satisfied with being limited to theoretical content coming from books that are years old." Cybersecurity education needs to be where students can get their hands on real-time stories, real-world data and make connections with 'in-the-trenches' practitioners, he added.

Another response, this time from a student, Callum Lake, highlighted problems surrounding the education of the end user. He explained that warnings are often issued about the re-use of passwords, for example, but the main problem is that people "don't see the loss of usability as a worthwhile compromise to the ease of using the same standard password."

> ***"The human factor is even more of a concern, and a heavy investment is needed in continuous cyber-education"***

Lake argued that cyber-professionals can talk endlessly about implementing secure behaviors and mindsets, but the end user simply does not care about the technicality behind such issues. "I've had countless arguments with people about how to be safer online and they just see it as me nagging," he said. "I feel that we don't get to the root issue and we don't approach it in the right way; we don't link [security] to users' personal lives."



24% of respondents cited the human element of security as a key trend

Another significant human-related issue highlighted is the gap that has emerged between business executives and security professionals, cited by Heath Renfrow. He argued that "cyber-professionals are struggling to adapt to their new ability to get their message across to business executives," and this leads to the need for better cyber-cultures. That push for culture, he said, must come from the very top of organizations.

Renfrow also said that, while he has seen investment in awareness and cyber-education tools rise steadily over the years, with the COVID-19 pandemic situation, "the human factor is even more of a concern, and a heavy investment is needed in continuous cyber-education."

It's also important to consider some other factors embedded in the human element of security, pointed out Lisa Forte, founder of Red Goat Cyber. For example, "emails being sent accidentally cause data breaches," which suggests failings both in technology, and in training.

Likewise, Rick Goud, CEO of Zivver, argued that awareness campaigns usually fail as "two weeks after receiving training, 80% of people have forgotten what they learned, so you need security strategies that work well in users' day-to-day duties and tools that are more effective."

No discussion on the human factors of security would be complete without considering the debate around whether the human is the 'weakest' or the 'strongest' link in security practices. As is tradition, there was a clear divide among responses regarding this issue.

Lake said that there is still a tendency to "call end users stupid" for making mistakes and he has seen too many incidents of people being told that poor security is their fault, "when in reality, we're not providing the right training and explaining it in a way that works for the general public."

Ayman El Hajjar assessed the human factor from a particularly interesting angle. He pointed out that "users are the weakest link, but we are researching how much training and awareness really is essential and whether the expectations we have of the user are too high – that we expect everyone to be an expert."

With some excellent points made and discussed, it's clear that the human element of information security remains an intricate and delicate topic. There may well still be too many ongoing problems with the type of language being used in the sector, issues with blaming users and ineffective training and mentoring, but ultimately, it is the user that keeps the industry alive, and that should always be remembered.

TREND FIVE: Phishing

– 18% of Respondents

Completing the top five most cited trends this year is the issue of phishing. According to 18% of respondents, phishing is playing a key role within the current cybersecurity landscape, particularly given the current situation regarding the COVID-19 pandemic.

Alan Woodward, visiting professor at the University of Surrey, said that in any crisis "we see an increase in the number of phishing attacks" and explained that many recent phishing threats were related to COVID-19.

One reason for this could be the amount of email traffic now flowing around the world. Ajay Arora said that the use of email opens up threats in a company's infrastructure, resulting in hackers trying to exploit new tools of remote collaboration. "Sophisticated phishing and impersonation are the first methods of attack," he warned.

Jason Nurse, lecturer at the University of Kent, added that the problem with phishing is around the nature of timing. In particular, attackers tricking users into clicking on the wrong things when they are not paying attention or are in a hurry. "Some of these [attacks] are nefarious and threaten to infect you if you don't pay up," he said, recommending that this is an area where training needs to be done so employees and users know what to look out for.

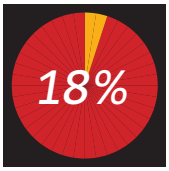
Woodward pointed out that even efforts made by governments to send out legitimate SMS messages warning people of potential scams can be exploited by cyber-criminals who have taken to using "SMShing" tactics to get people to click on malicious messages.

Senior security lead Gregory Parfitt explained that he has recently seen a "significant uptick" in the targeting of new starters within organizations, with scammers noticeably using impersonation emails claiming to be from the company CEO.

Nicola Whiting, CSO of Titania, said that successful attacks in this area are often undertaken "by more sophisticated actors" who are "believable enough to impersonate a known contact and convince their victim to initiate a wire transfer."

Likewise, Kevin Curran, professor of cybersecurity at Ulster University, explained that phishing efforts are becoming more sophisticated, and in the case of current phishing attacks against financial institutions, they are very customized. "They are designed to be effective in these environments by targeting large numbers of employees of financial institutions. The goal is to infect and compromise enough users so that the attacker can get end-to-end control of financial transaction approval systems, allowing them to initiate and approve transactions that appear to be properly authorized," he said.

Curran claimed that these attacks often use tailored techniques, dynamic websites and regularly updated methods. "The result is a series of attacks that have an alarmingly high success rate, yet a relatively low detection rate."



Completing the top five most common trends is phishing, cited by 18% of respondents

Clearly, phishing remains a significant data security threat and can be used by both 'basic' and more sophisticated attackers. So what are the best strategies for prevention and mitigation?

Rick Goud said that many businesses use email gateways and create rules to determine which emails are permitted to get through, but as attacks become more intelligent, better mitigation is needed. "Organizations need to make decision-making stronger as people often don't learn, rules are not specific enough and threats bypass rules."

Researcher Dr Arun Vishwanath argued that the role of the user, or recipient, is one that is important when it comes to phishing, in particular in user reporting as "organizations want users to report phishing, but if you look at the trends from the latest Verizon *Data Breach Investigations Report,* reporting numbers remain very low."

Other options like the DMARC standard are also available, whilst Chris Pierson, founder and CEO of Blackcloak, said "education continues to play a critical role in trying to bridge the gap in knowledge that exists, but there is still a divide in controls that will solve this problem in an automated and scalable way."

Phishing, he continued, is too easy to carry out as it is often straightforward to manipulate users. That is why, after all these years, phishing remains a threat vector and the only malicious 'tool' that made our top five trends.

FURTHER TRENDS

In total, 34 trends were cited by respondents in our research this year. Some of those are outlined in the upcoming single-mention trends section, but below are the remaining trends that make up our top 10. Just missing out on our top five, these topics proved popular enough to deserve their own special mention.

Compliance

– 16% of Respondents

Just missing a place in the top five for the first time since we launched this report in 2018, compliance came in at sixth place. Our upcoming section, SECTOR FOCUS: Practitioners, Vendors and Analysts, explores this topic in greater detail, but there has been a clear shift in attitudes towards the importance of compliance and regulation in 2020.

Internet of Things

– 14% of Respondents

The Internet of Things was cited by 14% of respondents, with those surveyed highlighting the security risks surrounding the continued rise in the number of IoT devices being used. Dr Chris Pierson, CEO and founder of Blackcloak, said "securing the ever-expanding numbers of IoT devices permeating the work environment is crucial," championing the need for automated detection of devices, identification of risks and device isolation.

Giovanni Vigna, director at the Center for Cybersecurity, UCSB and professor at the University of California, Santa Barbara, added that vulnerability analysis is one of the hottest trends in the academic world, and this was "largely a result of the blossoming of the IoT, which has brought to market a number of embedded devices with poor security and large deployments."

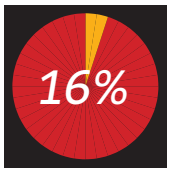
> ***"Securing the ever-expanding numbers of IoT devices permeating the work environment is crucial"***

Nation State Attacks

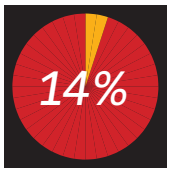
– 14% of Respondents

A number of respondents cited factors such as corporate espionage and financially-motivated cybercrime as key trends, as well as specific nation state attacks. Raj Muttukrishnan, professor of security engineering and director of the Institute for Cyber Security at City University, said that cases of state sponsored attacks "will grow exponentially due to the global political unrest that we are seeing today." To combat them, he advised, more focus is needed on predictive analytics and forecasting.

Furthermore, BitSight CTO and founder Stephen Boyer highlighted how challenging it is for private companies to defend against nation state attacks. "Everyone has security gaps, but imagine an SMB trying to fend off a sophisticated nation state attack – it is very difficult," he said. Boyer argued that SMBs can only focus on "locking the door and doing the basics."



The trend of compliance was cited by 16% of respondents



Internet of Things is significantly impacting the security industry, according to 14% of respondents

Adoption of New Technology

– 13% of Respondents

This trend, in ninth place, somewhat mirrors last year's most popular trend – the need for better and more secure technology – with respondents this year citing the necessity of security by design and more intelligent technology. Entrepreneur Joseph Chukwube said he views the biggest driver of cybersecurity as being "the fast adoption rate of new technology innovations versus the slow adoption of the proper security measures."

He claimed that most businesses are quick to implement new technologies, "but they are slower and more reluctant when it comes to employing the right security tools and measures to make the technology safe and secure."

Ken Pentimonti, principal at Paladin Capital Group, agreed, adding that resilience is achieved only through investment in a full spectrum of technologies that enable, monitor, manage and defend digital infrastructure.

Patch Management and Cyber-Hygiene

– 13% of Respondents

Many of the comments we collected cited the trends of cyber-hygiene and patch management – which have a natural synergy – and we've combined them here. Associate Professor Arun Vishwanath said cyber-hygiene is an important security issue, specifically with regards to how organizations measure it.

Investor and board advisor David Billeter voiced a similar view. "I think there's a growing realization that without good cyber-hygiene there's limited value in spending large sums on new tools," he argued.

> ***"Everyone has security gaps, but imagine an SMB trying to fend off a sophisticated nation state attack – it is very difficult"***

SINGLE-MENTION TRENDS

Whilst our research this year has shown that there are many themes and topics deemed to be of high importance to whole groups of respondents rather than individuals, it was interesting to see a handful of topics cited just once, each by only one person. There were five of these, and they are listed below:

- Weak passwords
- Whistleblowers
- Network monitoring
- Network segmentation
- Autonomous vehicles

This list of single-mention trends is shorter than that of last year's report, which had a total of nine. Notably, none of the single-mention trends in 2020 are the same as those from 2019, indicative of the constantly-evolving and adaptive nature of the information security industry.

One individual predicted that whistleblowing would become more common, adding that "drastic political action as a consequence of rapid changes in society will mean that insider threats become an even bigger risk."

With regards to the trend of autonomous vehicles and their security implications, a respondent said this is a topic gaining notable levels of interest. The key challenge here is the ability to detect and fix security vulnerabilities as vehicles become more complex and connected.

The final single-mentioned trend we will further analyze is that of weak passwords. Authentication as a general topic was cited by seven respondents in this year's research, but each of those mentions focused on factors such as identity management and next-gen authentication methods in the enterprise. However, for one of our survey cohort, the "brute forcing of accounts with weak and guessable passwords" is a significantly important issue, as "adversaries commonly target accounts where users have selected weak or guessable passwords in order to gain access to systems, services and network resources."

SECTOR FOCUS

New for this year's report, we have broken down the data to analyze it in regards to three specific verticals. Of the 75 people interviewed, one third were venture capitalists (VCs), investors and entrepreneurs (25); one third were academics (25) and the final third were cybersecurity practitioners, vendors and analysts (25).

By breaking down and classifying the responses of these three sectors, we have been able to understand the differences in priorities between sectors and also identify which topics and trends are most relevant to each individual sector. This allows greater visibility of the impact of different factors in different facets of the infosec industry.

VCs, Entrepreneurs and Investors

In total, there were 28 different trends cited by 25 respondents in this category, with the impact of the COVID-19 pandemic on information security (cited by 12 respondents) considered the most important. This was followed by the cloud and Artificial Intelligence/Machine Learning (AI/ML) – each cited six times – and the concept of Zero Trust, mentioned by five individuals. Interestingly, among this subset of respondents, 14 different trends were cited just once.

Focusing on the issue of Zero Trust, Ajay Arora, founder and COO of BluBracket, said: "Zero Trust will quickly accelerate its adoption to eventually replace VPN-based methods" as the classification of assets becomes even more important.

Arora added that security teams will realize that they cannot secure everything in this new world, but "tying identity in a Zero Trust system with classification will deliver organizations' need for secure prized assets."

Saj Huq, director of LORCA, concurred with Arora about the growing importance of Zero Trust, something businesses are becoming more interested in. In particular, he highlighted software-defined perimeters and networking, which Huq described as enabling a "perimeter-less environment."

Imran Ghory, partner at Blossom Capital, also spoke of the insider threat aspect of Zero Trust, referring to risky insiders as typically being rogue employees or those who unintentionally bring a compromised device into the workplace. "You cannot just assume everything on the network is safe" and Zero Trust makes life more practical, he added.

Another popular trend among respondents in this subset was that of the cloud. Olav Ostin, managing partner of TempoCap, said that if you're using several different versions of a product, you can struggle to keep all versions supported with updates. However, through a cloud-based solution, it's easier to effectively manage updates and patching.

> *"Zero Trust will quickly accelerate its adoption to eventually replace VPN-based methods"*

Ostin also argued that the "one-off cloud license is completely dead" now, suggesting a genuine future for cloud-only technology options going forward.

Practitioners, Vendors and Analysts

The second subset of data we will further analyze collates responses from security practitioners, vendor representatives, industry analysts and specialists.

In this cohort, a total of 27 trends were cited by the 25 individuals surveyed. Among these, both the impact of COVID-19 and the cloud were the most popular with eight responses each, whilst phishing, the human factor of security and compliance gained four responses each – with 11 single trends also referred to.

It is interesting to note that the topic of compliance, which was cited as the most important trend in the 2018 report and the third most influential last year, failed to make the overall top five in 2020, coming in at sixth place and only cited by 16% of those surveyed.

One would be forgiven for therefore assuming that compliance is considered 'less important' in 2020 than in previous years, despite the fact that significant, new regulatory frameworks have been introduced this year (the California Consumer Privacy Act, for example).

It is likely that a distinct lack of fines for data security and privacy failings over the last two years has played a significant role in this evolution of mindset. Steve Durbin, managing director of the Information Security Forum, surmised concerns about whether new regulations and international agreements are actually sufficient to fully address the issues powered by advances in technology.

Nonetheless, some respondents from this particular subset held firm to the belief that compliance remains a highly important driver of information security. For example, Heath Renfrow, director and CISO of the Crypsis Group, said that the impact of new privacy laws would cause "a significant increase in cybersecurity budgets" because of the impact of new frameworks, which he argued "have put to the forefront the need for a robust cybersecurity posture."

Similarly, Jeff Valentine, CTO at CloudCheckr, highlighted a heightened focus on governance and compliance checks, which are among the most common guardrails put in place. "For sensitive data, like consumer information and health details, we're finding that the most advanced organizations now have these security tools built into their processes rather than afterthoughts," he added.

> *"You cannot just assume everything on the network is safe"*

What's clear is that, although the topic of compliance remains one of interest to security professionals, on the whole, it is not regarded by individuals with the same importance as it has been in years gone by.

Education and Academic Institutions

The third and final subset of responses we will further analyze assesses feedback from individuals in the educational sector – both those teaching cybersecurity and related subjects, and those studying. *Infosecurity* would like to take this opportunity to thank the Association for Computing Machinery (ACM) for its assistance in gathering data.

In this subset, a total of 26 trends were cited by the 25 people surveyed. Among these, the topics of AI and ML proved the most popular, cited by 11 of the respondents. The human factor came in second place with 10 responses and the cloud scooped third with eight. A variety of other trends were also cited, including the prevalence of ransomware.

Professor Alan Woodward, visiting professor at the University of Surrey, argued that ransomware is still the most common form of cyber-attack. He drew particular attention to the rise of crimeware-as-a-service where cyber-criminals offer a "malware supply chain which continues to evolve."

Shawn Davis, adjunct industry professor at the Department of Information Technology at the Illinois Institute of Technology's School of Applied Technology, explained that he recently ran his own survey of 50 security professionals to establish the key factors driving the need for better security. One of the top five trends, he said, was "improved response regarding ransomware attacks."

Another trend – one that was cited by five people within this particular subset – also proved to be of interest. This was the topic of cryptography, encompassing Blockchain, quantum computing and advanced encryption.

Chaminda Hewage, associate professor in the Department of Computer Science at Cardiff Metropolitan University, declared "robust and tamper-proof services through distributed technologies such as Blockchain" an important emerging trend. Likewise, Raj Muttukrishnan, professor of security engineering and director of the Institute for Cyber Security at City University, referred to Blockchain as a market driver for several verticals, due to the inherent built-in security that comes with it.

With regards to more advanced encryption methods, Muttukrishnan said that, with quantum computing slowly becoming a reality, there is a threat to traditional cryptographic techniques, so there is more focus on applying the homomorphic technique to perform computation in encrypted domains.

> ***"Large scale quantum computers will defeat most currently deployed public key cryptography systems"***

Professor Keith Martin from the Information Security Group at Royal Holloway, University of London, concurred that whilst quantum computers may not yet be immediately on the horizon, the need to defend against them is arising now.

Brent Waters, professor at University of Texas, Austin, also agreed, recognizing a strong awareness and interest in developing cryptography systems against quantum machines.

"Large scale quantum computers will defeat most currently deployed public key cryptography systems" he said, but lattice-based cryptosystems and symmetric key primitives (such as AES) are believed to be secure against quantum attacks.

"I am not in a position to judge whether a quantum-factoring attack on large numbers is 10 years or 100 years away, but I can say that people are beginning to take it more and more seriously," he argued.

Waters also said there is a greater interest in the deployment of what he called "advanced cryptographic solutions" – including multi-party computation, attribution-based encryption and fully homomorphic encryption.

It was fascinating to hear such in-depth and insightful opinions around emerging cryptographic methods from the subset of educational respondents, perhaps evidence of academia's famous thirst for knowledge and innovation.

CONCLUSION

This report outlines many of the numerous and varying trends currently impacting the information security industry. It also demonstrates some of the deducible differences between individual sectors with regards to how certain trends are perceived.

Infosecurity's primary objective embarking on this research was to highlight the most important factors driving the information security industry in 2020. The unprecedented impact of the COVID-19 pandemic claimed its place at the top of that list. The crisis has greatly changed the way organizations work and secure their data, exposing businesses and users to vast new challenges, risks and threats.

However, if we consider the impact of the pandemic to be an anomaly, it's clear that the other top trends in this year's research – the cloud, human factor, artificial intelligence/machine learning and phishing – represent nothing new from previous years, suggesting the industry is still being majorly influenced by recurring factors.

Whilst the omission of the topic of compliance from the top five most-cited trends is notable, the fact that the human element of security once again proved popular suggests that the sector has yet to breach the human usability and skills issues that have been so prevalent in recent years.

It has been a pleasure to bring this latest instalment of *Infosecurity's* industry report to you and we hope that it has proven to be an insightful piece of research reflecting on the current state of the information security sector END

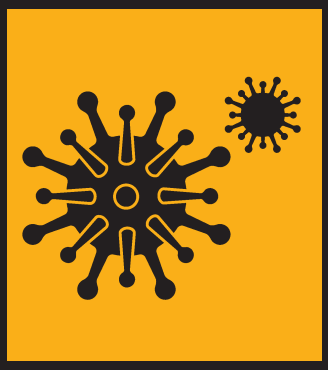
> ***"Infosecurity's primary objective embarking on this research was to highlight the most important factors driving the information security industry in 2020"***

ALL TRENDS

Trends are listed in order of most referenced

- **COVID-19's impact on cybersecurity**
- **Cloud, Security-as-a-Service and edge computing**
- **Artificial intelligence and machine learning**
- **Human factor**
- **Phishing**
- **Compliance**
- **Nation state attacks**
- **Internet of Things**
- **Adoption of new technology**
- **Patch management and cyber-hygiene**
- **Data privacy**
- **Zero Trust**
- **Authentication**
- **Crypto and quantum computing**
- **Board communication**
- **Ransomware**
- **Deepfakes and fake news**
- **Supply chain security**
- **Configuration and orchestration**
- **Brute force attacks and privileged access management**
- **Industrial Control System attacks**
- **DevSecOps and 'shifting left'**
- **Container security**
- **Threat intelligence**
- **Vendor relations**
- **BYOD and unmanaged endpoints**
- **Asset management**
- **Credential stuffing**
- **Cyber insurance**
- **Weak passwords**
- **Whistleblowing**
- **Network monitoring**
- **Network segmentation**
- **Autonomous vehicles**

Key Takeaways



The COVID-19 pandemic is the most influential trend impacting the information security industry in 2020

The evolution of the cloud is driving innovation whilst also exposing organizations to new security and privacy challenges

The human element of security remains key with regards to communication, learning, skills and fault-blaming

The trend of compliance is considered less influential in 2020, after being the most important (in 2018) and the third most important (in 2019)