ONCISOMEDIA
SOMEDIACO
IACONSUMPT
CONSUMPTIO
NSUMPTIONC

Content attracting the CISO community

CYBER THEORY

RESEARCH REPORT // Q3 2019

INTRODUCTION

2019 entered the history books as cybersecurity broke into the top 5 global threats to business continuity for the first time ever, according to PWC's 2018 Global CEO Survey.

While over-regulation clung to the top global threat spot, and global terrorism jumped from twelfth to second followed by geopolitical uncertainty, cybersecurity climbed all the way from tenth into the fourth position on the global threat ladder.

Ironically in North America, arguably the leaders in global technology bullishness, the region's CEOs actually ranked cybersecurity as the number one threat to business continuity. This owes largely to technology-related developments where CEOs expressed anxiety over both the promise and perils of artificial intelligence as it's applied to cyber-risk and the defense against cyber-attacks.

And joining in history-making events, it appears that the modern CISO has finally earned recognition as the sole business leader upon whom board members and C-suite executives must reliably depend to mitigate the now critical security threat and to set the security tone and vision for their companies.

While preventing, detecting and responding to cyberthreats and meeting compliance requirements have been well-established duties of the CISO, the rapidly evolving business opportunities accruing from digitalization and cloud computing are now expanding the threat landscape and creating increased reliance on the CISO in an evolving corporate leadership capacity.

In addition to deploying advanced secure technical architectures, implementing innovative countermeasures to combat advanced threats, and rolling out security policies and standards that will keep the organization safe, CISOs are now being asked to address a tighter integration with business objectives and to move toward the management of enterprise cyber-risk and the creation of a shared cyber-risk ownership culture with the line of business (LoB) owners.

This is no small feat and combined with the scarcity of experienced CISO talent, it is the impetus behind the unprecedented expansion of compensation packages, often into the millions, for competent and visionary CISOs.

In this, our launch issue of CyberTheory, we will explore the current and future state of cybersecurity, the key issues driving the shift in the corporate board room perception of cyber-risk and add substantive analysis to what we believe are the most engaging topics in the space.

The data behind our findings is summarized and abstracted from tens of thousands of interactions and activities we track with participating members across our global digital network of 30 online media properties, and provides valuable indicators of relevant topical interest for both solution providers and security practitioners alike.

This report will be published quarterly and will reflect upon the evolution of the constantly shifting cybersecurity landscape. We hope you find it useful and welcome you along for the ride.

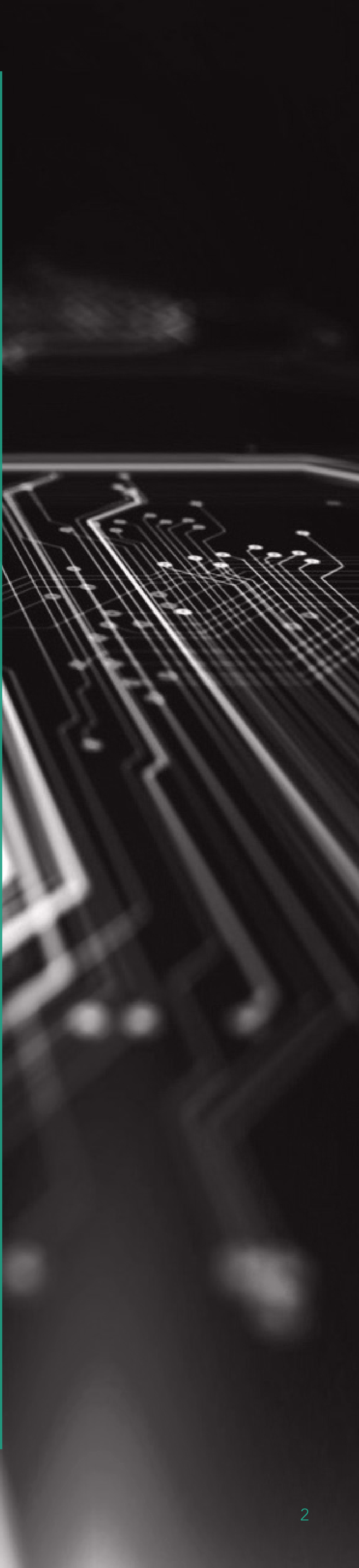


TABLE OF CONTENTS

TIME FRAME

Among the hundreds of data breaches that occurred during the third quarter of 2019, we learned that between the high-profile breaches at Facebook and Zinga, more than 637 million customer records were stolen, the major delivery brand known as DoorDash was hacked to the tune of 4.6 million customers' PII, and 44 separate healthcare data breaches were reported, exposing PHI data from 710,279 patients.

In September, AIG reported that the largest source of claims under its cybersecurity insurance policies was from business email compromise (BEC) attacks, followed by ransomware, and that the total number of cybersecurity claims filed last year doubled, with 2018 claim dollars eclipsing the total amount of all the claims filed in 2016 and 2017 combined. This news has serious implications for the insurance industry as it tries to balance the risks of largely anecdotal actuarial threat data against the attraction of doubled cyber-insurance premium margins compared to standard P+C policies.

The HIPAA Journal reported in August that the number of people affected by the huge data breach at the American Medical Collection Agency is nearing 25 million customers and that 23 healthcare organizations in the country have been affected by that breach. Healthcare continues to lead the way as the least prepared and most targeted industry sector begging the question of when and how the sector will step up its game before IoT vulnerabilities spread to the point where actual lives are at risk.

Imperva, a leading provider of internet firewall services that help Web sites block malicious cyberattacks, announced a security incident with its Cloud Web Application Firewall that exposed sensitive information of an unspecified number of customers. Another cybersecurity firm, SpiderSilk, also announced in August

2019 Major Breaches

June 19, 2019

AMERICAN MEDICAL COLLECTION AGENCY

Incident & Breach Response

Discovered when a disproportionate number of credit cards that had interacted with AMCA's web portal were later associated with fraudulent charges.

July 30, 2019

CAPITAL ONE

Cloud Security

The FBI identified and arrested a former AWS employee, Page A. Thompson, whom they alleged to be the perpetrator of a data breach affecting 100 million customers.

LAPD

Third-Party Access

The Los Angeles Police Department begins investigating a possible data breach that appears to have exposed the personal information of about 2,500 full-time officers, as well as records related to 17,500 potential police candidates.

"3,813 cybersecurity incidents were publicly reported during the first six months of 2019, an increase of 54 percent over the same period in 2018."

- Risk Based Security

that one of their servers supporting their MoviePass client containing 161 million full credit card customer records was left unprotected on the web.

These two incidents, combined with multiple AWS-related container breaches, added fuel to the growing suspicion that the very companies that were supposed to understand and have addressed the fundamental issues surrounding cybersecurity protection are unable to walk the walk.

In the same 3-month period, State Farm announced that the PII of an undisclosed number of customers' records were compromised in a "credential stuffing" attack; Marriott International disclosed it's taking a $126 million charge due to the breach of its Starwood reservations database that exposed the records of 383 million guests, including passport and credit card information; and of course, the mother of all Q3 breaches, Capital One announced that their data breach affected more than 100 million customers, while the FBI identified and arrested a former AWS employee, Page A. Thompson, whom they alleged to be the perpetrator.

CapitalOne was apparently one of more than 30+ other AWS customers whose records were allegedly stolen by Ms. Thompson and that breach may also become historic in that it raises serious questions about liability, criminality and insurability that will be addressed in subsequent months as the investigation unfolds.

Other high-profile breaches involved stolen Social Security numbers and complete dossiers of police department applicants at the LAPD; a ransomware attack on City Power in Johannesburg, South Africa; the loss of 100 million plus records at Evite; the breach at an unspecified number of patient genealogy records on unprotected AWS servers that included gene-based health information at Vitagene, a DNA-testing service; and payment card information for 5.3 million cardholders in 35 states scraped from compromised point-of-sale systems at gas pumps, coffee shops, and restaurants owned by Iowa-based Hy-Vee, which operates more than 245 supermarkets in the Midwest. That payment card data is now for sale on the dark web.

In related news, Equifax announced that it had settled the FTC data breach actions against it for $700 million, and painful fines were levied against British Airways for £183 million and Marriott for $123 million. These actions, in spite of what many believe to be a mere wrist slap against Equifax considering the weight of their negligence, offer solid evidence of the growing trend for the imposition of serious penalties for failure to properly protect and defend customer data.

Finally, in August, Risk Based Security released their 2019 mid-year data breach report finding that 3,813 cybersecurity incidents were publicly reported during the first six months of 2019, an increase of 54 percent over the same period in 2018. In addition, these incidents exposed over 4.1 billion records, which was a 52 percent jump over the previous year. If there was ever any doubt as to whether things were getting better or worse, this report provides ample evidence that the state of affairs in cybersecurity is declining.

(2019 continued)

August 8, 2019

STATE FARM

Credential Stuffing Attack

PII of an undisclosed number of customers' records were compromised in a "credential stuffing" attack.

August 28, 2019

IMPERVA

Cloud web application firewall

A security incident with its cloud web application Firewall exposed sensitive information of an unspecified number of customers.

September 27, 2019

DOOR DASH

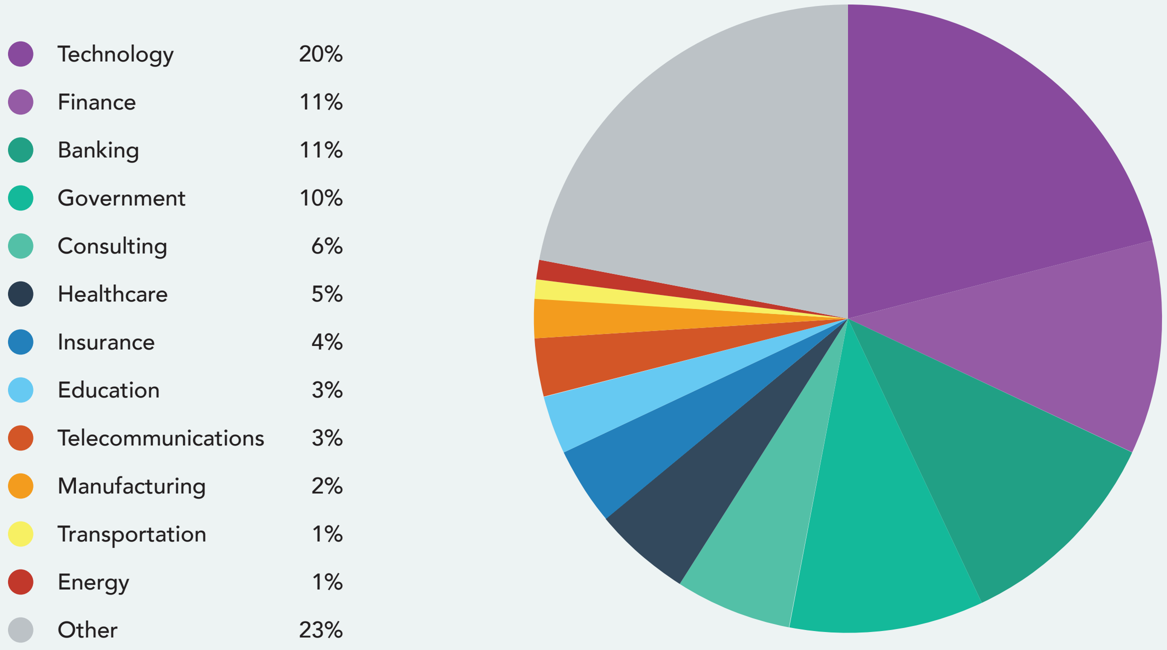
Third Party Access

4.9 million customer, contactor and merchant records were breached after "unusual activity" by a third-party service provider.

INDUSTRY BREAKDOWN

It may seem like common sense for organizations to properly position and support the security leader to succeed, but it's not common practice.

CISOs BY INDUSTRY SECTOR



●	Technology	20%
●	Finance	11%
●	Banking	11%
●	Government	10%
●	Consulting	6%
●	Healthcare	5%
●	Insurance	4%
●	Education	3%
●	Telecommunications	3%
●	Manufacturing	2%
●	Transportation	1%
●	Energy	1%
●	Other	23%

Other includes: Vendor, Pharmaceutical, Retail, Utilities, Legal, Media, Not For Profit, Engineering, Automotive, State Government, Hospitality, Chemicals, Marketing & Advertising, Biotechnology, Food & Beverage, Entertainment, Real Estate, Shipping, Communications, Credit Union, Environmental, Electronics, Federal Government, Construction, Apparel, Agriculture, Recreation, Machinery

As you can see from the distribution of CISOs by industry sector, not all industries share the sense of urgency or belief in the criticality of the CISO role. Finance, banking, technology and government all share in varying degrees the view that putting an effective CISO in charge of information security is a business necessity. Banking and most financial services companies operate under structured regulatory requirements with which they must comply, so boarding and supplying a CISO with the tools to succeed seem to be no-brainers for these segments.

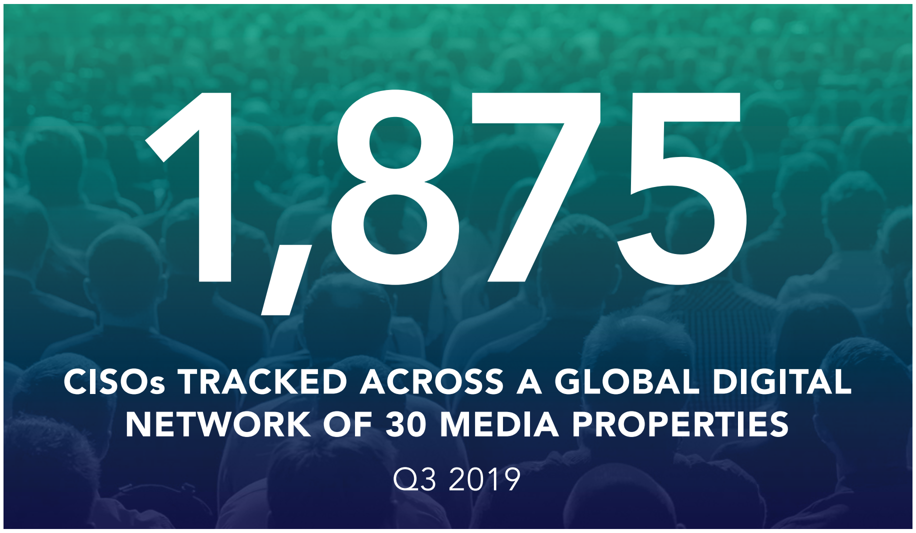
Conversely, sectors like education, telecommunications and manufacturing are less prone to strict cybersecurity regulations and tend not to focus very seriously on the requirement for mature cyber-risk management. Given the popularity of ransomware attacks on the education sector in 2019, this trend may soon change.

It remains puzzling, though, when healthcare, a sector that operates within a strict regulatory framework, exhibits a poor track record for hiring strong CISOs yet continues to remain among the most targeted industries for cyber-attacks. While financial institutions must carefully protect customer PII, health organizations have a more complex duty of care with regard to PHI, medical surgical devices and robotics, and much greater liability exposures compared to most other industry sectors.

Nonetheless, we find that healthcare tracks at less than or equal to half the CISO distribution when contrasted with its counterparts in technology, banking and government. We expect that as healthcare attacks continue to increase, this trend will also begin to reverse.

IMPENDING CISO CHALLENGES

The intersection of legacy IT and modern cloud technologies has created a hybrid world where centralized computing is shrinking as most critical workloads are shifting to the edge. This evolution presents a heightened challenge among the 1,875 CISOs we tracked.



1,875

CISOs TRACKED ACROSS A GLOBAL DIGITAL NETWORK OF 30 MEDIA PROPERTIES

Q3 2019

At the same time, every major technology and regulatory trend is pushing a similar narrative that challenges business to create a digital-ready IT infrastructure.

The key to accelerating digital transformation is ensuring a secure eco-system that can support a direct and private traffic exchange between key business partners, while removing the distance between IT services, systems, applications, data and clouds and their customers.

As pressure continues to mount from C-suite executives and LoB owners, the modern CISO must rapidly assemble the tools, processes, policies and organization that can stay ahead of the demand, while avoiding the risk potholes along that road. Among the most difficult today are cloud, Kubernetes, docker APIs and edge computing. In the near future, CISOs will have to contend with IoT, blockchain and quantum computing.

As we have seen repeatedly during the last 90 days, our commercial cloud service providers have assembled a technologically sound infrastructure that enables customers to leverage part of the digital transformation equation, but the implementation processes have remained flawed at best. The recent sensitive cloud data exposures at Starbucks, Netflix, Electronic Arts, TD Bank, Ford and Imperva, and the massive breach of Capital One, are not good indicators that customers are ready to execute a cloud computing strategy with even the premier cloud vendors, let alone local or hybrid solutions.

In each case, human error was the culprit behind the vulnerability. Unfortunately, these errors aren't isolated incidents and are more common than they should be. Until the industry gains control of the entire process, any expectations of leveraging digital transformation will be blocked by the stubborn realities of technical complexities.

Industries that are dependent upon secure interconnections for digital transformation include telecommunications which represents almost 20% of all interconnection bandwidth, as interconnection is central to their future business, enabling new digital business services and last-mile scale for 5G technologies.

Cloud and IT Services are a leading consumer of interconnection bandwidth and are expected to grow at a robust 40%+ CAGR, as they extend their global reach and their hybrid multi-cloud infrastructures.

Banking and insurance ride the wave of a perfect digital storm, with the convergence of fintech, cybersecurity, data compliance and new competitive ecosystems enabling the industry to compete in an expanding digital marketplace.

Manufacturing, traditionally a physically distributed industry, looks to digital restructuring for new efficiencies, services and revenue streams. Manufacturing alone is expected to consume 12% of all interconnection bandwidth.

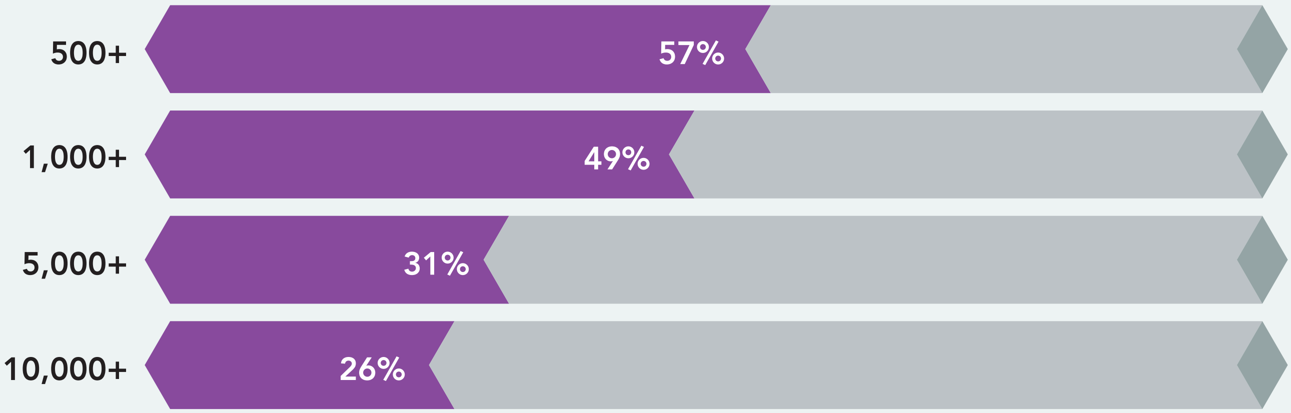
In order to harness the opportunities inherent in digital transformation, businesses will have to increase the speed with which they adapt to the enabling technologies and the processes that support strategic execution. The cybersecurity maturity of an organization typically correlates to the length of time it has been leveraging the tools, technologies, people and processes required for proper cyber-risk management fundamentals. That correlation maps to the time it takes to build cyber-risk expertise that can enable success. It doesn't happen overnight, and it certainly doesn't happen at the pace with which the current demand requires.

The next 5 years will create interesting challenges at the confluence of cybersecurity and digital transformation.

COMPANY SIZE BREAKDOWN

According to a recent study by Gartner, worldwide cybersecurity spending growth will jump by 8.7% this year, to $124 billion.

COMPANYS SIZE (EMPLOYEES) OF CISOs TRACKED



The top drivers are the need for improved detection and response capabilities, compliance with privacy regulations like GDPR and CCPA, and the ability to address increasingly advanced digital business risks (IoT, AI/ML, big data, blockchain, quantum computing, etc.).

Gartner also predicts that security services will account for 50 percent of all industry cybersecurity budgets by 2020, followed by infrastructure protection and additional network security hardware. The shift in spend toward security services is a response to the severe talent shortage most companies face and the regulatory-compliance-related need for external third-party experts for help in specialty areas like identity and access management (IAM), identity governance and administration (IGA), and data loss prevention (DLP).

As C-suite executives recognize that secure digital transformations can yield better customer experiences and richer digital services, they are now beginning to support cybersecurity spend in initiatives like security by design and SecDevOps that had not been previously funded.

While we have tried to benchmark cybersecurity spending through firmographics related to industry or company size, we find that defining cybersecurity spend isn't easy. We have seen reports of budgets dedicated to cybersecurity varying by as much as 300 percent in three major studies from some of the biggest insights firms.

However, we have found reliable point benchmark data in a recent survey by Deloitte and the Financial Services Information Sharing and Analysis Center, that characterized banks, insurance companies, investment managers and other financial services companies spending between 6% and 14% of their annual information technology budget on cybersecurity, for an average of 10%. This equals roughly 0.2% to 0.9% of company revenue.

Benchmarks aside, the macro view supported by ISACA's State of Cybersecurity 2019 report and Gartner research suggests that budgets for cybersecurity are increasing by an average of 8.7% this year, a sizeable increase over the same metric for general IT spending, which is estimated at 3.2% in 2019.

While this indication of a spending increase is encouraging, we don't believe it is enough to keep up with cybersecurity mandates related to the speed of digital transformation impacting all business in 2019 and beyond.

NETWORK OVERVIEW

Our global digital network monitors industry-, topic-, and region- specific media properties, all focused on information security and risk management. These properties accumulate millions of page views per month and in total track nearly 1 million security professionals.

One of the significant observations from data monitored over the last quarter is that the leading type of breach continues to be PII (personally identifiable information), and to the extent that a business stores and/or processes this type of data, those businesses will become cyber-attack targets regardless of size.

This breach category represents 97% of all cyber-attacks in Q3.

The stolen credential attack vector accounted for 34% of all intrusion access and also led to malicious actors taking over other critical accounts. Name and physical address (49%) and personal health information (46%) were the second and third most commonly compromised type of data.

Community banks, small financial services firms, hospitals and small healthcare groups were hit more often than larger enterprises in these sectors in the last 3 months. The volume of unauthorized access attacks indicates that we are not doing a very good job of managing identity and access management controls, or insisting upon two-factor authentication, one-time passwords, or physical tokens.

According to the Ponemon Institute and Keeper Security, two-thirds of SMBs suffered a cyber-attack in the past 12 months. If an SMB has been lucky enough to slide into that minority 33% who avoided an attack, the odds are not good that it will remain safe two years in a row. In the current era, 6 out of 10 SMBs report the attacks they're witnessing are becoming more targeted, increasingly sophisticated and more difficult to prevent.

While the current estimate of the cost of a data breach for SMBs is $117,000, the true costs have been averaging as much as $3 million over the last 12 months.

This number would appear high on the surface, but most SMBs tend to think of the attack costs and report them purely in terms of the ransom amounts and direct damages while forgetting to factor in the extended costs of sustained system outages and business disruption. In most cases, downtime is the most significant impact following a breach. The economic fallout that downtime can impose on organizations in sales, marketing, manufacturing and finance is not trivial.

All data indicates that SMBs are increasingly becoming prime targets for PII that can be appended to other identity profile information collected from larger company breaches in an attempt to create high-value dossiers. Smaller businesses across all industry sectors are affected and can no longer ignore the need to harden their assets and defenses against progressively complex and sophisticated attack vectors.

ACTIVITIES TRACKED

Email remains the channel of choice for CISOs. Despite the digital marketing experts long predicting the demise of this communication channel, our data points prove the exact opposite.

Considering the advent of more real-time digital social targeting in the digital space, and extreme competition for the CISO's attention, we have actually seen clear traction and growth by focusing on targeted messaging via email.

Traditional inbox outreach through content aligned to persona needs seems to give the most amount of control to CISOs, allowing them to pick and choose which messages to prioritize as well as filtering items for later review. As the world's first main-stream digital filing cabinet, we do not see email losing steam any time soon as one of the most reliable, efficient CISO acquisition and nurture strategies.

TOTAL CISO ACTIVITIES TRACKED

20,282

EMAIL OPENS

42%

EMAIL CLICKS

34%

PAGE VISITS

24%

ASSET DOWNLOADS

35%

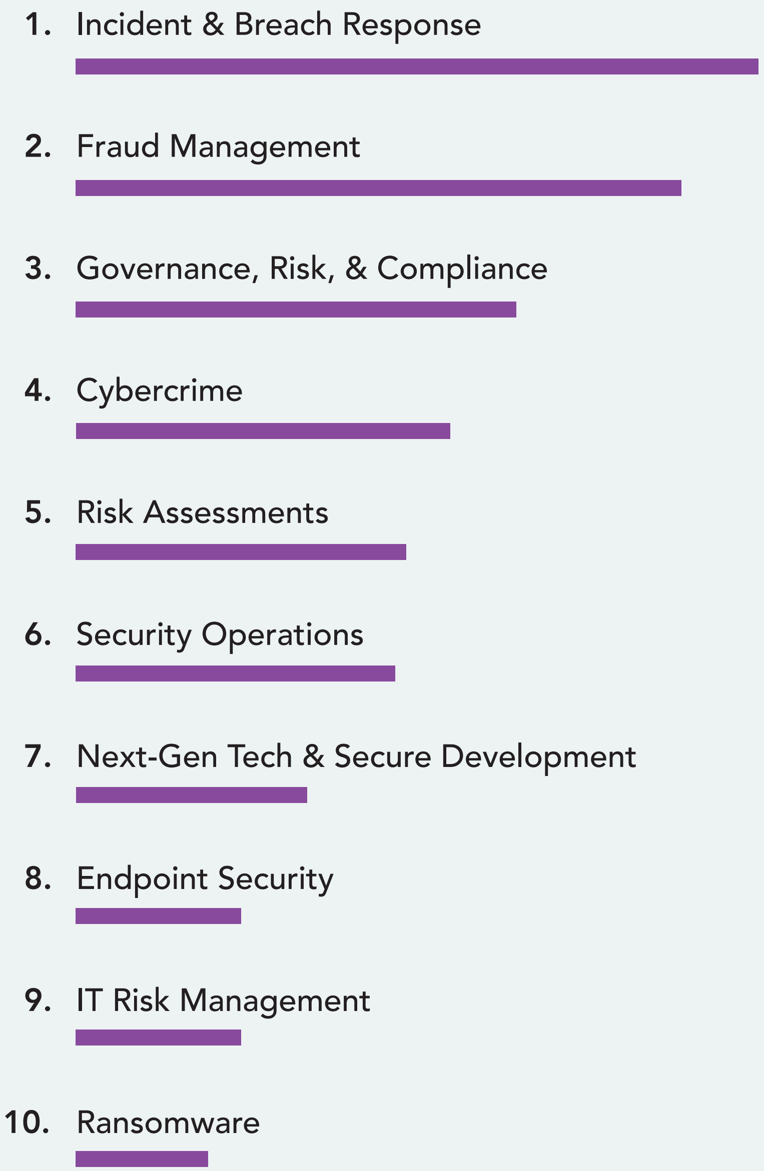
MOST ENGAGING CONTENT TOPICS

The topics that most interested our CISO audience during the quarter were incident and breach response, fraud management, governance and risk management and cybercrime.

Given that one of the most egregious breaches in history occurred during Q3, it is not surprising that those topics would get so much traction. The CapitalOne breach raises several significant issues around cybersecurity that run the gamut from the mechanics of the breach itself, the security and reliability of cloud service providers, the extent of negligence liability claims that may arise, the potential impact on cyber-insurability for companies of CapitalOne's size, along with some human interest issues related to mental health in the workplace.

We expect to see expanded coverage of the CapitalOne breach well into 2020 as each one of these issues becomes an informative and cautionary story unto itself.

MOST ENGAGING TOPICS FOR CISOS



MOST ENGAGING CONTENT TYPES

We track the activity of 1,875 CISOs who participate with us in events, surveys, interviews, roundtables and panel discussions. Because we have established trusted relationships with most of these industry leaders, we believe our research most accurately reflects the realities of issues and topics around which the community at large is concerned.

What we find is that beginning with editorial content around the most active topics, our audience dives deeper into whitepapers, webinars and in-person events which we produce throughout the year that develop the narratives, technical details and back-stories around these topics to fully reveal the relevance to their own environments and the specific information security exposures and challenges.

Our goal, by combining all of this rich topical research, is to bring to our audience a quarterly review that continually provides up-to-date analysis, trends and news that are most relevant and actionable to the entire InfoSec community while assuring that the content is informative and entertaining at the same time.

EDITORIAL CONTENT

59%

WHITE PAPERS

13%

WEBINARS

18%

3,352/quarter

INTERVIEWS

6%

1,151/quarter

*Percentages from 1,875 CISOs tracked

TOP CONTENT PIECES

A surge in scanning attempts by attackers to locate and exploit known flaws in SSL VPNs manufactured by both Fortinet and Pulse Secure became the most compelling content that CISOs were following in Q3.

With 480,000 Fortinet FortiGate SSL VPN endpoints connected to the internet, it is clear why CISOs would be concerned. The unpatched flaws enable malicious actors to steal passwords and gain full access to corporate networks. While it isn't clear how many Fortinet VPNs are unpatched, reports that 14,000 of the Pulse Secure SSL VPN endpoints are in fact unpatched is enough to unnerve most CISOs.

Coming in right behind that is the story we did on the use of manipulated digital fingerprints to avoid fraud detection systems. These modern-day versions of carding are effective at tricking even advanced anti-fraud systems' verification mechanisms into believing that a criminal perpetrator is a legitimate user.

Our reporting on the surging business email compromise (BEC) scams captured the third spot on our CISO topic list. BECs are now costing U.S. companies a total of more than $300 million a month and the specific case of a Nigerian businessman allegedly carrying out an $11 million business email compromise scheme on a U.K. affiliate of U.S. Caterpillar was compelling in that it illustrated so clearly the mechanics of what is also called CEO fraud.

We will continue to work hard to bring you the most comprehensive reporting each quarter on the top events impacting global threat and cyber-risk vulnerabilities. Our objective is to provide thoughtful insight and analysis into the most relevant issues surrounding the business of cybersecurity protection, management and defense.

Top Editorial Content

1. Hackers Hit Unpatched Pulse Secure and Fortinet SSL VPNs
2. For Sale on Cybercrime Markets: Real 'Digital Fingerprints'
3. FBI Arrests Nigerian Suspect in $11 Million BEC Scheme
4. Apple iPhones Hacked by Websites Exploiting Zero-Day Flaws
5. Texas Says 22 Local Government Agencies Hit by Ransomware
6. Why Did Federal Agencies See Fewer Breaches in 2018?
7. Fake VPN Website Delivers Banking Trojan
8. Paige Thompson Charged With Hacking 30 Organizations
9. 80 Indicted for Scams, Including Business Email Compromises
10. Cloud Security: Mess It Up and It's on You

Top Vendor Content

1. Resiliency Orchestration with Cyber Incident Recovery
2. Blind Spots in the Threat Landscape
3. Hard Truths about Account Takeover and Strategies to Defend Your Enterprise
4. Multi-Factor Authentication for Dummies
5. Five Key Technologies for Enabling a Cyber Resilience Framework
6. 10 Incredible Ways You Can Be Hacked Through Email & How To Stop The Bad Guys
7. Do the Benefits of Personal Devices at Work Outweigh the Drawbacks?
8. Hard Truths about Account Takeover and Strategies to Defend Your Enterprise
9. AI for Cybersecurity
10. 40 Questions You Should Have in Your Vendor Security Assessment

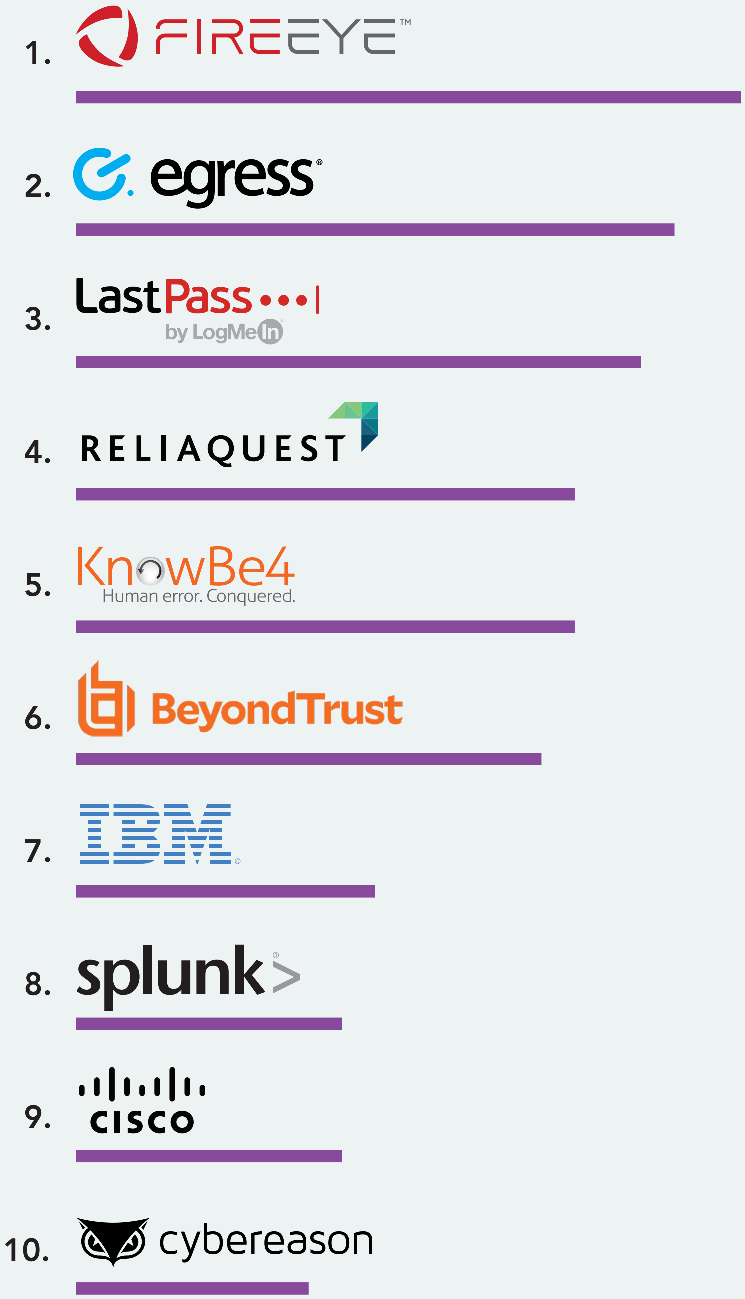
TOP BRAND ENGAGEMENTS

Account takeover protection, network security and behavioral analytics, email security, password security, unified threat detection and security awareness training led the list of popular topics based on the most sought-out vendors we tracked through Q3.

This topical interest maps well to the most dangerous real-world vulnerabilities and exploits that have led to most of the breach activity we tracked during that same period. CISOs are clearly on the right track as shoring up identity theft protection and defending against credential stuffing will go a long way toward reducing the threat landscape at most organizations.

In addition, strengthening network threat detection capabilities and implementing comprehensive security awareness training are both keys to improving our overall cybersecurity postures and raising the bar against cyber-attacks and malicious threats.

MOST ENGAGING BRANDS FOR CISOS



MOST ENGAGING TOPICS - IN-PERSON EVENTS

CyberTheory analyzed data from the ISMG network and dozens of CISO/Executive Roundtables in Q3. While RSA and trade shows, conferences and summits are highly useful events for initiating discussion around topics of interest, CISOs are gravitating toward intimate, smaller, much more topically focused events.

Executive Roundtables afford more time and exploration of a topic with far greater granularity and experiential insights from CISOs, other industry thought leaders, vendors and market analysts providing analysis and exploration that goes beyond the natural limits of larger venues.

Based on our analysis of all data from this past quarter, the top 10 most popular themes were:

1. Vulnerability Management

Which may owe in part to the recent kick-off of "the year of vulnerability management" by the Cybersecurity and Infrastructure Security Agency and its upcoming binding operational directive (BOD) on vulnerability disclosure policy.

2. Cloud Security

Likely the result of the upsurge of vulnerabilities in container software (up 240% in the last two years) and the risk-management issues that have surfaced around shared responsibility models.

3. Digital Transformation

Being driven by line of business infatuation with realized productivity and profitability gains while at the same time ignoring the dramatic increases in associated risk.

4. Virtual SOC

Gaining traction as an attractive alternative to the dedicated SOC model due to the move away from a dedicated facility, ability to staff with part-time contracted resources and its reactive nature enabling ignition upon a critical alert.

5. Zero Trust

An approach to cybersecurity that assumes anything inside or outside of a corporate network, including data, devices, systems and users, is a security risk and must be checked and verified before being granted access, is gaining traction as the most viable cybersecurity strategy.

6. Industrial IoT

A popular topic as the increased reliance on networked industrial systems is creating significant risk for conducting business in the digital age and as industrial IoT (IIoT) takes shape, locking down data and systems ranging from networks and communications to clouds and devices is becoming a significant challenge for everyone.

7. Privacy

An active topic owing to the combination of new regulations and the growing need to classify data by risk and to ensure that the data is protected is one fraught with strategic business, legal and technological complexity.

8. Endpoint Protection

A growth segment within the cybersecurity markets that includes malware prevention, data security, mobile and zero-trust framework alignment has caused an uptick in interest among CISOs searching for a comprehensive enterprise endpoint security solution that can address these expanding zero-day attack vectors.

9. Third-Party Risk

The combination of increased cybersecurity incidents related to third-party vendors, regulators focusing on supply chain risk and pressures from increased economic volatility is driving escalated interest in this threat category.

10. DevSecOps

And finally, an interest in implementing security from the start has taken center-stage with the advent of agile development and the recognition of the need to change the underlying DevOps culture to embrace security as a methodology without exception.

SPECIAL RSA CONFERENCE COVERAGE

From humble beginnings in 1992 as a specialized conference focusing on cryptography, and it's imminent challenges in the digital realm, the RSA Conference has now broadened its reach to encompass all aspects of information security for almost every kind of practitioner and vendor.

The RSA Conference is arguably the largest and most important security trade show series in the world. With flagship events in both the United States and APAC, over 50,000 security professionals will directly participate in person, along with hundreds of thousands of other security professionals tapping into conference content via the official RSA Conference website and other media outlets. With over 500 sessions and 700 speakers, you can be sure the who's who in security will be in attendance every year.

Each year, media partners will provide extensive coverage of the conferences. Through video interviews, audio interviews, and the written world, hundreds of pieces of original content are produced and promoted online. These editorial-led pieces will typically revolve around insight from security practitioners, CISOs, analysts, law enforcement involved with cybersecurity, and executives from cybersecurity vendors.

CyberTheory tracked the content produced from two RSA Conference events in 2019 – the U.S. event which took place in March, along with the APAC event which took place in July – published to a worldwide digital network of media brands focused on cybersecurity. CISOs were tracked as they accessed each piece, and what follows is an overview of the most accessed pieces along with commentary as to seemingly why each piece was so popular.

POST MEDIA INFLUENCE

Cyber extortion. GDPR compliance. The state of cybersecurity education. GRC. Automation in cyber risk management. Metrics for cybersecurity effectiveness. We strive to bring you timely, relevant coverage of these and other topics.

McAfee's John Fokker (center) and Raj Samani (right) participate in a video interview with ISMG's Mathew Schwartz.

For example, our in-depth interview with McAfee's Raj Samani, their chief scientist, and John Fokker, their head of cyber investigations, on the topic of cyber extortion, garnered more than doubled the attention given to the other leading topics.

The fascinating interview drilled down into the face of modern crime, unwrapped the latest extortion schemes, explained the business model behind the leading ransomware in the extortion space, and described how they can be managed through an initiative called nomoreransomware.org, which enables victims of ransomware to retrieve their encrypted data without having to pay the criminals.

Another topic garnering strong interest is the issue around GDPR guidelines for notifying governing authorities of a breach. An interview with Brian Honan who heads BH Consulting in Dublin, consults with Europol and founded Ireland's first computer emergency response team, sheds definitive light on the topic.

In addition to determining if a breach warrants notification, he explains why every organization that must comply with GDPR should make use of ENISA's (the EU Agency for Network and Information Security) breach impact methodology, what regulators want and don't want to see from breached organizations, and the risk organizations face if they get it wrong.

Popular as well was the interview with Brad Topchick, the managing director of Mooreland Partners, who is a leader in the cybersecurity investment advisory and M&A space on the health of the cybersecurity marketplace today, the business trends that are driving that growth and the technologies underpinning the most interesting innovation.

Topchick points out that the market is now $130 billion and shows no signs of weakening as more than $15 billion in venture capital has been invested in new technology startups during the past 5 years. He discusses the major M&A deals and their impact on the marketplace from NTT's acquisition of WhiteHat to AT&T's purchase of AlienVault to Symantec's acquired inclusion of Luminate into their expanding family of cybersecurity products.

With the explosive growth in AI/ML and deep learning, Topchick sees a robust future in both innovation and capital expansion.

MOST POPULAR RSAC COVERAGE

The Art of the Steal: Why Criminals Love Cyber Extortion
McAfee // 60,000 views

GDPR: Data Breach Notification 101
BH Consulting

Women in Tech: How Are We Doing? How Should We Be Doing?

Investment Adviser's View of Cybersecurity Market
Mooreland Partners

The Future of Cybersecurity Education - Part 2
Intel Corp

GRC: A Status Report
LogicGate

Measuring Security Effectiveness in a Dynamic Threat Landscape
Verodin

Cyber Risk Management: Why Automation is Essential
Skybox Security

Minimizing Automation Bias in Machine Learning
Microsoft

Are Autonomous Vehicles Trustworthy?
Argo AI // 20,000 views

INTENT BY TOPIC

CyberTheory's access to a wide network of digital properties has long been integrated with powerful analytics platforms. We monitor vendor activity across the editorial network and analyze topics of interest. This first-party data, also known as intent data, is segmented by our marketing operations team across various data points to enhance account-based marketing.

More recently, our partner network of websites has begun combining their own proprietary first-party data collection with the third-party data co-op platform Bombora. This enables us to get a more accurate and complete picture of intent by account across the entire web. The Bombora platform collects data from thousands of related, high-value media properties, including Gartner, G2Crowd, and Forbes. When the accounts being monitored engage with content on those sites, Bombora can indicate that they are surging on a particular topic.

We analyzed the content categories accessed by all trackable employees from the 10 organizations with most activities recorded by their corresponding CISOs, the results are below.

Intent data is highly valuable as it can be the missing link in improving sales outreach and creating highly tailored communications.

ORGANIZATION	Cybercrime	IAM	Cybercrime aaS	Threat Intelligence	Insider Threat	Breach Response	Critical Infastructure	Cyberwarfare	Fraud Risk Management	Application Security	SIEM	PAM	ID Theft	Governance	Dev Sec Ops
National Geospatial Agency	x					x		x							
Commerzbank Capital Markets Corporation						x				x	x				
JM Finn & Co		x			x							x			
Naval Postgraduate School	x												x	x	
BMW Financial Services	x	x		x											
State of Texas Emergency Management Agency	x		x												x
American Express	x			x	x										
ACME Federal Credit Union		x		x			x								
Citizens Bank	x		x						x						
BNP Paribas	x	x	x												
Total Heat	70%	40%	30%	30%	20%	20%	10%	10%	10%	10%	10%	10%	10%	10%	10%

CLOSING THOUGHTS AND LOOKING FORWARD

As we have indicated through our research during the past quarter and patterns we saw emerge at this year's huge RSA Conference, some of the hottest topics have been the privacy imperative now facing organizations, lessons learned from GDPR notification processes, the legal and operational complexities unfolding from the Capital One breach, and the fact that cyber extortion - and especially more advanced phishing techniques - seems unstoppable, as does the continuing threat of U.S. bank card fraud.

Through extensive dialogue with experts from industry and law enforcement, we have shared their latest insights into cybersecurity awareness and upskilling, as well as how law enforcement and the FBI are combatting election interference attempts and social propaganda spread and will continue to do so as the 2020 political campaign season heats up.

We have interviewed CEOs, CISOs, analysts, researchers, law enforcement agents and educators, with topical discussions ranging from cybercrime to risk management, DevSecOps to cloud security, VPN security to business email compromise and every latest and persistent threat and risk challenge facing the industry.

These topics continue to map to the areas in which we have seen increases in vulnerability over the last three quarters, like the expansion of the threat landscape through mobile and IoT, the frequency of cloud container compromises and server misconfigurations, and the continuing growth of ransomware as a formidable threat vector now fueled in part by new cyber-insurance underwriting practices.

Moving forward, we expect to see the growth of topics around issues like ransomware, data privacy – tools, regulation, policy and process, identity management, DevSecOps – secure application development and quality, approaches to closing the skills gap and the continuing expansion of diversity in the cyber-workplace.

We also expect a new set of challenges that will emerge around issues related to cloud computing security and breach liability, a redefinition of insider threat, the evolution of officer and board member fiduciary liability, new regulations around demonstrated proof of care and preparedness, adjustments to and perhaps the elimination of large cap cyber-insurance tower coverages, new threat vectors emanating from AI and ML advances and technological response to IoT and hardware level threat and risk management.

If it's happening and you care about it, we will continue to bring it to you each quarter with extensive editorial coverage in CyberTheory, the media research resource that you can count on in a dynamic and rapidly changing world.

For more details on the data from this report and our findings, please contact us: content@cybertheory.io or visit https://www.cybertheory.io/contact/.

CYBER THEORY

We are a full-service cybersecurity marketing advisory firm. We constantly collect and analyze the latest customer data segmented by security practitioner, industry, and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona.With strategic insights from global education services, media providers, intelligence analysts, journalists, and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompass all aspects of cybersecurity as well as the related fields of fraud, audit, compliance, and risk management.

(212) 518-1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018 • www.cybertheory.io