
CISOMEDIA
MEDIACONSUMPTION
Content attracting the CISO community
CYBER THEORY
RESEARCH REPORT // Q4 2019

INTRODUCTION

The last quarter of 2019 saw cyberattacks rise to the number two position among the top 10 global threats to doing business according to an October survey by the World Economic Forum.

The evidence of evolving attack vectors by criminals and state-sponsored actors has dominated mainstream media coverage during the last three months of 2019. In tandem, the corresponding data from our digital and in-person events has shown a dramatic increase in engagement by the world's top CISOs.

A compounding factor that is fueling the concern is the recognition that the adoption of digital business models is changing corporate threat profiles. Increased dependencies on cloud computing, and expanded supplier access to enterprise IT systems pose more risk than ever. According to October's WEF Executive Opinion Survey, corporate leaders in advanced economies ranked cyberattacks as the number-one risk for businesses in the US, Canada, the UK, France, Italy and Germany. Even among emerging market countries, where issues like mass unemployment and the inadequacy of physical infrastructure dominate the political conversation, cyberattacks remain among the top ten threats.

When taken as a whole, fiscal crises, global warming, natural disasters, energy cost, and other unforseen catastrophes, all paled when compared to the threat of cyberattacks. This steadily increasing acknowledgement of the cyberattack threat to business in contrast to our current economic stability presents new business opportunities for agile technology and services vendors.

As you will see in this report, the CISO activities we analyzed in the last three months were dominated by topics relating to 3rd Party Risk Management, Next-Generation Technologies & Secure Development, Virtualization & Cloud Security, Cybercrime and Identity & Access Management, mapping to both the incident data we observed in the quarter and the top threats recognized by global business leaders.

There's no surprise our CISO interactions increased by almost an order of magnitude over the 3rd quarter of last year as we tracked more than 178,000 queries across our 30 media properties, analyzed 837 asset downloads and correlated the activities of 3,388 CISOs actively engaged in our network.

In this, our second issue of CISO Media Consumption, we will continue to explore the current and future state of cybersecurity, the key issues driving the shift in the C-suite and boardroom perception of cyber-risk, as well as add substantive analysis to what we believe are the most engaging topics in the space for the ultimate cyber decision maker: the CISO.

TABLE OF CONTENTS

TIME FRAME

Among the hundreds of data breaches that occurred during the fourth quarter of 2019, many were the consequence of unsecured server configurations (several severe Elasticsearch exposures), over-provisioned access privileges, and more sophisticated phishing schemes that lured gullible employees lacking proper cyber threat awareness.

October (our National Cybersecurity Awareness month) kicked off the 4th quarter with a successful phishing attack on the Gary, Indiana-based Methodist Hospital network where through two compromised email accounts, cyber-thieves were able to access and steal 68,039 patient records.

Among the data elements captured were patient address, date of birth, Social Security number, driver's license number, state ID number, passport number, medical record number, CSN number, HAR number, Medicare number, Medicaid number, diagnosis information, treatment information, health insurance subscriber, group, and/or plan number, group identification number, financial account number, payment card information, electronic signature, username and password. Methodist Hospitals continues to review its security policies and procedures and is implementing safeguards to improve defenses against phishing attacks in the future.

Despite being placed in the top quartile for data security readiness by a third-party firm, Kalispell Regional Healthcare discovered in October that they too had been breached as the result of an email phishing campaign that successfully lured employees to offer their system login credentials. This breach offered up PHI on 130,000 patients including patient's name, Social Security number, address, medical record number, date of birth, medical history and treatment information, and health insurance information.

In October, the Adobe Cloud's 7.5 million users discovered their email addresses, usernames, location, Adobe products, account creation dates, dates of last login, subscriptions and payment status exposed in an online unprotected database. Adobe blamed the incident on a misconfiguration to one of its "prototype environments" that led to the cloud server becoming exposed in the wild. Adobe fixed the problem and issued a statement acknowledging that the data could have been accessed or downloaded but claimed it was unclear whether any of it had been. The good news was that the details didn't contain passwords or payment data. The bad news is that with all that other data, fraudsters could easily spam users into revealing both as well as spear-phish Adobe Premium users, hijacking their high-value Creative Cloud accounts and offer them on dark web markets.

Finally, Network Solutions revealed in October that it was hacked again, causing users to reset their passwords. But according to the giant domain registrar, no credit card data was apparently compromised and by now, users are probably getting used to it.

Rounding out the month were breaches at Mercedes-Benz, 3 million PII records at UniCredit, Kaiser Permanente, ZenDesk, NordVPN and a compromised credential attack at Avast, the Czech-based antivirus giant, which allowed access to 400 million customer records on their network. The investigation is "ongoing."

In November, Facebook quietly revealed another privacy breach involving around 100 developers who were able to access customer data through over-provisioned access privileges on what should have

2019 Q4 Major Breaches

October 8, 2019

METHODIST HOSPITAL

Phishing Attack

Through two compromised email accounts, cyber-thieves were able to access and steal 68,039 patient records.

October 22, 2019

KALISPELL REGIONAL HEALTHCARE

Phishing Attack

An email phishing campaign successfully lured employees to offer their system login credentials resulting in the breach of 130,000 patient records.

October 25, 2019

ADOBE CLOUD

Cloud Security

7.5 Million users discovered their email addresses, usernames, location, Adobe products, account creation dates, dates of last login, subscriptions and payment status exposed in an online unprotected database.

been restricted servers. Facebook claims the problem was fixed and no data was stolen or mis-used. We also learned that another cybersecurity industry leader, Trend Micro announced a security incident that led to the theft of PII data from 120,000 customers resulting from a disgruntled insider accessing a customer support database. The data was then used to conduct scams involving telephone solicitation of customers from fraudsters pretending to be Trend Micro employees attempting to extract payment data for special promotions.

In addition, November brought us The Gekko Group, a hotel management company with 600,000 hotels across the globe, who confirmed that it had leaked over 1 terabyte of personal data belonging to customers, and more than a million accommodation provider clients and partners. This breach was caused by one of the most common and recurring errors these days, the failure to password protect an Elasticsearch database upon which the information was stored. This makes it super-easy for cyber-criminals because anyone who found it online could simply access it without setting off any security alerts.We saw the exact same condition result in the exposure of 57 million Cathay Pacific customers data one year earlier.

Another huge Elasticsearch exposure joined the crowd in November when an unprotected server containing 1.2 billion records of PII data was found lying open on the Internet with 622 million unique email address, social media profiles, phone numbers, employers and job titles. This data, representing a comprehensive amalgam collected from B2B lead-generation companies' lists, was being used for highly effective, targeted phishing attacks, business email compromises and identity theft campaigns.

Credit cards and passwords are one headache, but when a victim's phone number and Facebook profile is leaked, the amount of work required to recover is non-trivial – imagine updating contact lists with new phone numbers and changing every two-factor account just because someone forgot to secure a server.

All of these Elasticsearch exposures, while not data breaches per se, bring up two growing concerns. One, is the question of liability for the originators and/or custodians of the exposed data, and two, even though the data is aggregated from "public sources", what is the impact on privacy rights and data protection from this form of data enrichment and where do liabilities lie, if any? We expect to see an increase in exposures, insurance and liability issues surfacing as 2020 unfolds.

Rounding out our November hit-parade are the breach at OnePlus, the Chinese smartphone manufacturer through an unpatched vulnerability in their customer website. Customer phone numbers, email addresses, first and last names, and shipping addresses were stolen, though the company has not yet clarified either the extent of the damage or the quantity of records affected.

And, T-Mobile, the multi-national wireless network giant, suffered a major data breach that affected over 1 million customers with the usual PII. Apart from the incredible inconvenience and identity fraud risk to its customers especially during the holiday season, T-Mobile's cybersecurity practices face increased scrutiny, and their deal value may suffer a significant hit (ala Yahoo) in preparation for their impending merger with Sprint.

The phishing threat continued into December with a high-profile series of breaches targeting Canadian banks. The attacks were executed by sending legitimate looking emails with a PDF attachment that included official bank logo and authorization codes required by the targets to renew their digital certificate for the online banking system. Clicking on any URL in the document redirected the victims to a phishing page that required the entry of their banking credentials. The phishing website resolved to a Ukrainian IP address.

Concluding our quarterly recap, we envision that achieving organization-wide threat awareness will be a top business priority in 2020.

(2019 continued)

November 5, 2019

FACEBOOK

Server Misconfiguration

100 developers were able to access customer data through over-provisioned access privileges on what should have been restricted servers.

November 21, 2019

GEKKO GROUP

Cloud & Web Application Security

1 terabyte of personal data was leaked, belonging to customers, and more than a million accommodation provider clients and partners.

December 4, 2019

SPRINT

Server Misconfiguration

A contractor mistakenly exposed cell-phone bills of 261,300 non-Sprint customers by loading the database into an AWS storage bucket which he had misconfigured and failed to password-protect.

December 19, 2019

FACEBOOK

Cloud Web Application Security

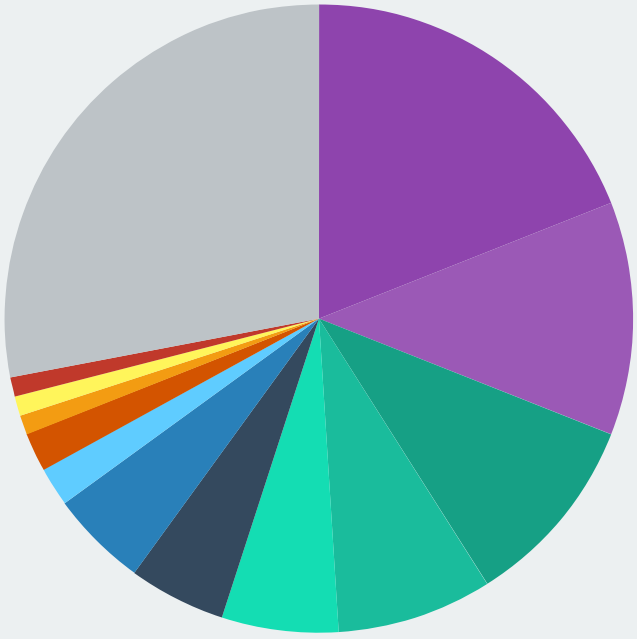
267 million users PII exposed online due to another unsecured Elasticsearch database.

INDUSTRY BREAKDOWN

Given the number of Healthcare breaches in the quarter, we envisioned a spike in interaction around phishing attacks throughout that sector, yet activity in Healthcare remained at around the prior quarter's level of 5%.

CISOs BY INDUSTRY SECTOR

Technology	19%
Finance	12%
Banking	10%
Government	8%
Consulting	6%
Healthcare	5%
Insurance	5%
Education	2%
Telecommunications	2%
Manufacturing	1%
Transportation	1%
Energy	1%
Other	28%



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 we can see from the distribution by industry sector, Technology, Finance, Banking and Government continue to represent the most interaction with CISOs during this past quarter. All of these industries share in common the need for compliance with structured regulatory requirements so, combined with the volume of compromised credential breaches we saw in Q4, it is not surprising that these sectors should be the most active.

Healthcare remains puzzling however, given the number of breaches in the quarter. The breaches at Methodist Hospitals and Kalispell Regional Healthcare would likely have touched off a spike in interaction around phishing attacks throughout that sector, yet activity in Healthcare remained at around the prior quarter's level of 5%, less than half of finance or banking.

Given that 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, we expect CISO activity to increase soon.

Insurance, telecommunications, manufacturing and transportation remained virtually unchanged since the third quarter while education fell off the top ten altogether.

This is interesting because with the frequency of Elasticsearch vulnerabilities exposed this quarter, we thought we would have seen a spike in activity from the Insurance sector in outreach toward gaining a better understanding of the emerging liability issues and approaches surrounding custodial duty of care.

Perhaps as this trend continues, the decade's first new quarter in 2020 will reflect an uplift of interest in data stewardship and C-suite responsibility for protection of assets across the board with a renewed interest in the energy, transportation and telecommunications sectors.

IMPENDING CISO CHALLENGES

As we have seen during the last 90 days, the majority of breaches stem from misconfigured servers, email compromises, phishing attacks and insufficient attention to fundamental security hygiene. One hard-to-dismiss takeaway is that skilled resource constraints and a general lack of security awareness are compounding existing gaps and even creating new vulnerabilities.

The world of the modern CISO hasn't changed much from last quarter. Complex threats from an expanding attack surface brought about by Cloud and Edge computing, and the explosion of APIs being leveraged to deliver data-as-a-service to both internal and external business partners, have created significant security management challenges.

Digitization and the rapid departure from central controls have extended the threat landscape well beyond the perimeter of the classic castle and moat defense, and quickly moved new security issues outside the purview of most CISOs.

In an attempt to stay abreast of these demands, CISOs are scrambling to assemble appropriate tools, processes, policies and organizational initiatives. Most find themselves overwhelmed just dealing with the day-to-day exposures resulting from increased pressure to leverage new technologies with increasingly faster adoption curves.

As we have seen during the last 90 days, the majority of breaches stem from misconfigured servers, email compromises, phishing attacks and insufficient attention to fundamental security hygiene. One hard-to-dismiss takeaway is that skilled resource constraints and a general lack of security awareness are compounding existing gaps and even creating new vulnerabilities.

The series of attacks that was discovered in December against a large group of leading Canadian banks, was a highly sophisticated and well-executed multi-channel phishing operation that had been running undetected since 2017. This demonstrates the level of planning and orchestration that cyber-criminals have now achieved. As forensics will soon begin to reveal the extent of the damages, security leaders are now presented with a glimpse into the near future of large-scale email impersonations, highly credible fake digital certificates and well-disguised yet fraudulent communication and transaction authorizations.

Many of the other notable breaches this past quarter were sourced in compromised credentials, insider attacks and over-provisioning of access privileges which underscore the need to focus on identity-centric, zero-trust security measures.

Even the relatively minor Facebook relied on improperly managed access privileges that enabled unauthorized and in this case, known developers to have their way with that data.

All of the personal data leaked in the various ElasticSearch discoveries not only in the last quarter but in the last couple of years, are due only in part to the fact that they lack built-in password protections and firewalls. We've witnessed PHI and PII leaks on 85% of Panama's citizens, 57 million U.S. citizens, 58 million Chinese citizens and 33 million businesses all due to these server configuration failures.

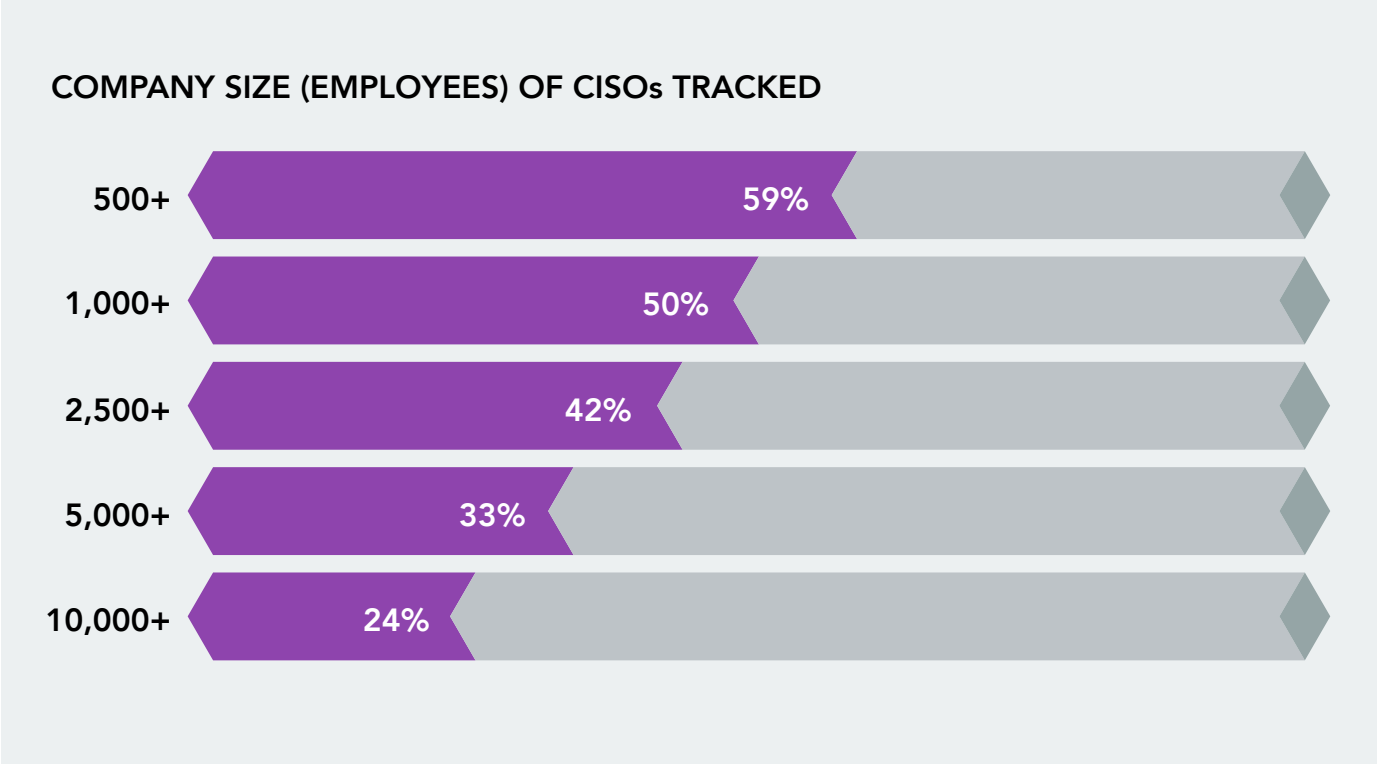
ElasticSearch is adamant about its server security and pointedly has recommendations about how to use secure authenticated sign-on, managed users and roles, encryption, layered security and audit logging to assure that their servers are properly configured against access vulnerabilities.

These exposures continue to comingle with the Cloud services shared responsibility model, our inattention to foundational best practices, and the need for increased vigilance around identity and access management.

In an era when anyone can claim to be anyone else on a network, identity access management has probably become the most important security control of all.

COMPANY SIZE BREAKDOWN

Larger enterprise CISOs delegate more of their research and diligence to staffers while they shift their attention to more strategic issues around organizational security integration and business enablement.



Based on our tracking this past quarter, the distribution of interactions when measured by company size hasn't changed very much since 3Q19.

The majority of CISO interaction again comes from security practitioners in companies with 500 to 1,000 employees trying to improve their tactical detection and response capabilities, their ability to comply with privacy regulations like GDPR and CCPA, and the escalating need to address advanced business risks and expanded attack surfaces attendant with business digitization and cloud computing pressures.

The issues don't change as the size of the enterprise increases, but frequency of interaction on day-to-day tactical topics appears to recede as larger enterprise CISOs delegate more of their research and diligence to staffers while they shift their attention to more strategic issues around organizational security integration and business enablement.

While it remains true that communicating directly with the CISO is a desirable outcome from marketing outreach, we find that increasingly, the direct reports to the office are more appropriate channels for tactical technology, service, process and educational proposals and pursuits.

Most CISOs today do not answer their phone, return voicemail or interact with email. Only upon the rare event that a piece of content, whether it be a white paper, blog post, use-case or product brief, webinar or podcast is sufficiently compelling, will the modern CISO actually respond to outreach.

More often than not however, the CISO's staff members who are tasked with the business of keeping the SOC running, investigating and responding to security incidents, maintaining network and end-point defenses, patching for known vulnerabilities and figuring out ways to prevent phishing attacks are the ones with the most to gain from frequent and regular vendor interaction and are in turn, the most responsive.

The quality of the content is key, however. Product and service vendors who focus on tactical solutions in the mid-cap spaces and create compelling content that tells their story are likely to engage with willing prospects searching for practical and proven technology and process that address their day-to-day challenges with use-cases that resonate.

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 every day.

The leading causes of breach in 4Q19 continued to be weak and stolen credentials, back doors and application vulnerabilities, phishing & social engineering, overly provisioned and misconfigured cloud servers, insider attacks and fundamental hygiene failure (patches).

The continued success of Ransomware attacks points to poor back-up and recovery processes and management, weak or non-existent network segmentation and monitoring, a lack of proper endpoint security defenses, weak authentication and credential management and poor security awareness.

Ransomware has had such impressive success in the quarter, that most of the attackers have moved exclusively on to public sector attacks, where according to the most recent data, Ransomware attacks finished the year by successfully targeted 948 government agencies (including schools and healthcare providers) in 2019.

Community banks, small financial services firms, hospitals and small healthcare groups continued to be hit more often than larger enterprises in these sectors in the quarter. Unauthorized access attacks spiked, underscoring the increased level of serious attention that needs to be paid to identity and access management controls, and moving toward some form of multi-factor authentication. The era of the common password is coming to an end.

Driven by the record prices being charged for medical identities on the dark web, healthcare continued to present the most attractive cyber-target for identity theft. We saw a dramatic resurgence of targeted ransomware attacks against hospitals, medical practices, and nursing homes and combined with third-party vendor breaches and phishing, healthcare data breaches continued to soar.

Ransomware damage by itself is estimated to reach $11.5 billion annually this year and $20 billion per year by 2021. Unsurprisingly, this type of year-over-year increase in anticipated damages makes ransomware the fastest-growing type of cybercrime in the past year.

The quarter gave no indication that the global cybercrime economy which has now grown to estimates of at least $1.5 trillion in profits each year, according to a study commissioned by cybersecurity company Bromium, is showing any signs of slowing down. In fact, if Cybercrime were a country it would have the 13th highest GDP in the world.

Based on what we've seen as causes, there is tremendous opportunity for vendors of fundamental cybersecurity solutions to enjoy long-term success in this environment.

ACTIVITIES TRACKED

The fourth quarter of 2019 witnessed a 7X increase in CISO engagement over the previous quarter.

The number of active CISOs on our 30 media properties almost doubled from last quarter, from 1875 CISOs for the 3 months ending 9/30/2019 to 3,388 for the 3 months ending 12/31/2019. What was most interesting was the order of magnitude increase in total activities in this very short time frame. As the political climate posed more cyber risk, there was increasing interest to not only learn about the latest news and insights but to leverage the latest solution-specific research for every business use case.

TOTAL CISO ACTIVITIES TRACKED

178,010

EMAIL OPENS

42%

EMAIL CLICKS

34%

PAGE VISITS

24%

ASSET DOWNLOADS

837

MOST ENGAGING CONTENT TOPICS

The topics that most interested our CISO audience during the quarter were 3rd party risk management, next-generation technologies & secure development, virtualization & cloud security, and cybercrime.

There's no surprise that 3rd party risk management tops this quarters list of most engaging content topics. We have heard great concern from our CISOs over how to protect their organizations from this growing sphere of contractors and other "privileged access" individuals. Unfortunately, these third parties may not always abide by some very elementary internal controls to secure data.

Financial institutions are increasingly relying on third parties to support mission critical operational functions, giving them access to some of the most valuable PII data, a goldmine for cybercriminals. As the push for a more seamless user experience to IOt devices, influences even the most conservative institutional adopters, managing this 3rd party risk will be critical. The topic of Next Generation Technologies and Secure Development jumped 5 places to the runner up this quarter, not a surprise considering the tense political climate, and the growing importance of intellectual property. And finally, virtualization and cloud security rounds out the top 3. In light of the high profile unsecured AWS and Elasticsearch exposures, it is understandable that interest in this topic remains strong.

MOST ENGAGING TOPICS FOR CISOS *

1. Third Party Risk Management
2. Next Gen Techologies & Secure Development
3. Virtualization & Cloud Security
4. Cybercrime
5. Identity & Access Management
6. Security Operations
7. Governance
8. IT Risk Management
9. Account Takeover
10. Anti-Phishing, DMARC

*From a selection of 100+ topics

MOST ENGAGING CONTENT TYPES

We track the activity of 3,388 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.

We've seen a growing appetite for long-form content this quarter. White papers are getting more detailed and hyper targeted to address very specific use cases serving information security persona interests. The power of content marketing allows CISOs to consume this research at their own time, place, and pace. In addition, a properly crafted white paper facilitates one of the first critical trust touchpoints in the sales cycle, validating proof of concept long before implementation. Our advisory team has been involved in the creation of assets of this type for years and they are highly prized among our audience, filled with valuable information addressing very focused problem/solution narratives. Essentially, the finished product combines hours of subject matter expert interviews in a condensed and easy to understand format.

EDITORIAL CONTENT

25%

WHITE PAPERS

44%

WEBINARS

23%

INTERVIEWS

4%

*Percentages from 3,388 CISOs tracked

TOP CONTENT PIECES

A security researcher uncovered what may rank as one of the most significant iOS weaknesses ever discovered: a flaw that enables bypassing the security protections present in most Apple mobile devices.This was the most compelling content piece CISOs were following in Q4.

With the recent controversy of law enforcement requesting backdoor access to iPhones, our top performing editorial piece was of great interest to CISOs. Even though the exploit required physical access to the device, it demonstrated a security paradigm shift for the iOs user universe. As more enterprises adopt bring your own device (BYOD) policies, this subject matter will continue to draw peak interest.

Microsoft's warning about their Bluekeep vulnerability came in a close second place. Even though cryptomining malware does not currently present a large threat to the enterprise, 700,000 windows systems remained unpatched, and there's been a growing concern that a more dangerous exploit will be developed by cybercriminals.

The Capital One breach is the cyber threat that remains on the radar of CISOs in various forms, even from not a strictly security perspective. In early November, we learned that the bank's CISO, Michael Johnson was being demoted and moved to an outside advisory role. The company is currently scouting for a new security leader. Job hunting anyone? Regardless if the shakeup of the bank's security structure is publicized or not, CISOs are taking notice and taking notes

Top Editorial Content *

1. Apple iOS Has Permanent Bootrom Vulnerability
2. Microsoft Warns Users: Beware of Damaging BlueKeep Attacks
3. Following Massive Breach, Capital One Replacing CISO: Report
4. Vendor Email Compromise': A New Attack Twist
5. T-Mobile Says Prepaid Accounts Breached
6. Attackers Demand $14 Million Ransom From IT Services Firm
7. Unsecured Server Exposed Records of 1.2 Billion: Researchers
8. Ryuk Eyed as Culprit in New Orleans Ransomware Outbreak
9. Microsoft Will Apply California's Privacy Law Nationwide
10. Two Uber Hackers Plead Guilty

Top Vendor Content *

1. How Another Firm's Breach Could Impact Your Organization
2. Making Security Part of the Business Team
3. Goodbye Legacy Technologies. Hello Zero Trust Network Access
4. How to Prevent 81% of Phishing Attacks from Sailing Right into Your Inbox with DMARC
5. Definitive Guide to Next-Generation Network Packet Brokers
6. Use Security Ratings to Achieve Your Security Goals
7. Third-Party Vendor Security and Privacy Risks - A Security Handbook
8. Put Those Cloud Security Objections to Rest
9. Mobile DevSecOps at Speed - The 5 Steps from Dusted to Trusted
10. The Surprising Ways that Inline Bypass Protects Business Operations

*From a content repository of 1000+ pieces

TOP BRAND ENGAGEMENTS

Network visibility and analytics, cloud security, cyber risk management, security suite software, and security awareness training led the list of popular topics based on the most sought-out vendors we tracked through Q4.

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. We have seen great interest in managing third party risk and securing the cloud.

With the alarming rise of unsecured Elasticsearch database and misconfigured AWS buckets, CISOs are clearly identifying with the vendors that provide the appropriate solutions and are interested in learning more about integrated security offerings and suites of software. Vendors offering awareness training services remains a critical area of interest this quarter. As 90% of attacks begin with phishing, it's becoming more important than ever that the workforce is properly trained and knowledgeable on these attack vectors, what they look like and how to prevent them.

We envision that achieving organization-wide threat awareness will be a top business priority in 2020 and vendors in this space will maintain a stable level of engagement for the CISO audience.

MOST ENGAGING BRANDS FOR CISOS *

1. Gigamon®
2. zscaler™
3. BITSIGHT
4. IBM
5. KnowBe4 Human error. Conquered.
6. OneTrust PRIVACY, SECURITY & THIRD-PARTY RISK
7. lastline™
8. riskrecon™
9. Akamai FASTER FORWARD
10. CYBERARK®

*Out of 100+ vendor brands on our global media network.

MOST ENGAGING TOPICS - IN-PERSON EVENTS

CyberTheory analyzed data from the ISMG network and from dozens of CISO/ Executive Roundtables hosted in Q4. While 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. Digital Risk Management/Cloud Security

We have heard great concern from our CISOs over how to protect their organizations from this growing sphere of contractors and other "privileged access" individuals. Unfortunately, these third parties may not always abide by some very elementary internal controls to secure the cloud.

2. 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.

3. 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.

4. Vendor Risk Management

There's been an increasing desire on maintaining vendor relationships for mission critical services while simultaneously minimizing third party risks. Many of our discussions have focused on successful use cases.

5. Threat Intelligence

Staying one step ahead of cybercriminals by learning their methods, gathering data on the dark web, and preparing for their attack vectors has been trending and presented as a cost-effective security strategy, resulting in some fascinating case studies.

6. Incident Response

Planning for a response following after a breach has become an inevitable part of security culture. From plan optimization, team coordination and communication, investigation, and recovery guidelines, this topic has seen a surge in CISO interest this quarter.

7. SOC Management

Closely connected with incident response, SOC management can make or break of a security strategy. Leveraging the most value from one's security operation's center has been a very important topical area for many CISOs.

8. 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.

9. DevSecOps

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.

10. Privacy & Security

And finally, 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.

CROSS THE IN-PERSON TO DIGITAL DIVIDE

Our proprietary data model has demonstrated how the most successful cybersecurity marketing is designed to provide a unified message across all channels, platforms and touchpoints. In a nutshell, it's been critical for vendors to provide a personalized one-to-one nurture regardless if the CISO is consuming content at in-person event or through a digital experience.

The power of live interviews can't be disputed. As part of building a content foundation, an in-person interview of a cybersecurity SME (carefully produced and executed) can cement business goals and precisely align them with content strategy.

Timing is everything and for content to be successful, it must not only keep up with market demands, it must provide personalized insight not available anywhere else. Getting inside the minds of industry leaders can be accomplished by aligning the right questions and answers in a narrative that provides both the business problem and solution: essentially a perfectly crafted story.

And like any good story, an in-person interview gets a life of it's own and can be a perpetual asset. Developing an 8 minute interview is rich enough to repurpose the core transcript text in as many as 4 blog posts, 10 social media engagements, 8 email communication narratives, as well as several animated explainer videos. For smaller marketing teams, this is a critical consideration as one can build a strategy to target leads as they move down the funnel with limited resources and time management

POST MEDIA INFLUENCE

Zero trust. Cyber resilience. Ransomware. AI. Cybercrime. We strive to bring you timely, relevant coverage of these and other topics.

Zero Trust

"Zero trust" was arguably the cybersecurity buzzword of 2019, but what exactly does it mean?

According to Jack Koons of Unisys, a speaker at a recent Information Security Group executive roundtable dinner and a featured presenter at the Dec. 3 Fraud & Breach Summit in Washington, there is no one-size-fits-all definition for the phrase.

"What is it? Is it a tool? Is it a capability? Is "zero trust" a philosophy about how you approach network security? Is it simply a philosophical journey with no endpoint? Or is it, yes, all of the above?" Koons goes into detail during his podcast interview.

Cyber Resiliency

Future trustworthy and secure cyber systems need to be able to operate even in a degraded state. Ron Ross of NIST details the components of a new publication on cyber resiliency.

Ross discusses how cybercrime is the "gift" that won't stop taking.

Prevention, Detection, and Response.

What can organizations do to improve prevention, detection and response in 2020? Ex-FBI leader MK Palmore of Palo Alto Networks shares his insights.

- The latest ransomware trends;
- Why organizations - even entire cities - keep falling victim:
- How to improve ransomware defenses.

AI and ML

Dena Bauckman of ZixCorp explains where the technologies are currently being used most effectively. Bauckman discusses:

- The difference between AI and ML;
- Where AI and ML are being applied today;
- Advice on selecting an effective AI/ML solution

MOST POPULAR COVERAGE *

Zero Trust': Can It Be Defined
Unisys // 60,000 views

Cyber Resilience at a Foundational Level
BH Consulting

What About Ransomware?
Palo Alto Networks

The Promise and Reality of AI and ML in Security Management
ZixCorp

Cybersecurity Leadership: The 2020 Vision
Cristopher Hetner

Cybercrime Support: Victory for the Midmarket
Cybercrime Security Network

How to Make Cyber Audits More Relevant
Mahindra Bank, General Mills, PCI

A CISO, a CIO and a CTO Discuss Cybersecurity Strategies
Edelweiss General Insurance, Reliance Jio, Wells Fargo

CISO Sizes Up Critical Technologies, Emerging Challenges
TMF Group

Applying AI and Machine Learning: Critical Steps
HDFC Bank // 20,000 views

* From an active content repository of 200+ video interviews for the fourth quarter of 2019

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.

In the 4th quarter of 2019, we saw a significant increase in content demand by the CISO persona. Our proprietary network of media sites recorded an increase of CISO engagement activity by 7x over the previous quarter. This increase has allowed us to have a very close and exclusive relationship with Bombora as the top tier publisher of the highest quality information security media. We currently enjoy the privilege of unrestricted access to the broader data set of actively engaged information security decision makers across the entire Internet landscape.

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	3rd Party Risk Mgmt	Account Takeover	Breach Response	Cybercrime	IAM	Next Gen Tech	Governance	Security Operations	Rasomware	Critical Infastructure	Application Security	Advanced SOC Ops	Fraud Risk Mgmt	Breach Notifcation
Arby's	x						x	x						
State of Maryland	x			x					x					
Royal Bank of Canada	x	x				x								
American Express				x	x					x				
US Army	x										x	x		
Sallie Mae		x	x		x									
BMO Financial Group	x	x											x	
Glenmark Pharmaceuticals			x	x										x
Blue Cross Blue Shield		x	x			x								
Foot Locker Inc.	x	x	x											
Total Heat	60%	40%	40%	30%	30%	20%	10%	10%	10%	10%	10%	10%	10%	10%

CLOSING THOUGHTS AND LOOKING FORWARD

As we have noted through both our research during the quarter and the focused interest expressed at events we engage with like the massive RSA Conference, the challenges associated with cloud computing, digitalization and risk, vulnerability and vendor risk management, industrial IoT and threat intelligence were the predominant issues on CISO's minds.

Microsoft warnings, CISO replacements, email compromise, unsecured servers, ransomware and Uber hackers dominated the CISO interest categories while third party vulnerabilities, zero-trust architectures, phishing attacks, next-gen packet brokers and security ratings led the way from the most consumable on the vendor content side.

We have interviewed CEOs, CISOs, analysts, researchers, law enforcement agents and educators, with topical discussions ranging from incident response to risk management, DevSecOps to SOC management, and every latest and persistent threat and risk challenge across all industry sectors.

These topics continue to map to the areas in which we have seen increases in threat activity over the last quarter, especially in third party risk management, virtualization, cloud vulnerabilities, identity and authorization, phishing and account takeover.

In the quarter to come, we expect to see continued growth of topics around issues like new forms of ransomware, the growth of data privacy regulations, identity, access and authorization management specific to industries like healthcare and financial services, advancements in tools to support DevSecOps, new approaches to email phishing detection, the application and implementation of deception technologies and practices to improve cloud server misconfigurations.

We also expect a new set of challenges that will emerge around issues related to third party breach liability, a redefinition of insider threat, the evolution of officer and board member fiduciary and personal liability, new regulations and fines directed at corporate proof of care violations, new threat vectors emerging from automated technology advances and various technological responses to IIoT threats and risk management.

If it's happening in cybersecurity and you care about it, our quarterly research report is where you'll read about it.

We will continue to bring the topics, trends, threats and technology advances that are of the most interest to CISOs with extensive editorial coverage, analysis and opinion in CyberTheory, the media resource that you can count on in a noisy, hyperbolic and dynamically 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/.

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