

Financial Services InfoSec Trends 2021

*How Financial Services Cybersecurity Leaders
are Guarding Their Companies Against the Latest
Information Security Threats*





Contents

Click below to navigate

Executive Summary

Criminals have always tried to rob banks. Online it is no different.

In this report, we investigate how cybersecurity executives are ensuring the integrity and availability of their companies' data in an environment of increased risk.

Inside, we highlight how financial sector cybersecurity executives have responded to a challenging year, characterized by the rapid change to a 'work from home' environment and an increase in attacks from cybercriminals.

Then, we highlight how these executives are

reevaluating their vendor relationships in the wake of the SolarWinds hack and the methods they are using to mitigate the risk of third-party breaches.

Along the way, you'll see at how financial sector cybersecurity executives are combating insider threats, securing endpoints and implementing zero-trust architecture.

With in-depth commentary from eight industry experts, it provides an essential snapshot of how cybersecurity executives are preparing to face the cyber threats of tomorrow. ■

Contributors



Raj Badhwar
SVP, Global Chief
Information Security
Officer, Voya Financial



Zsuzsanna Berenyi
Cyber Security
Awareness and Culture
Expert at London Stock
Exchange Group



Steve Jump
Director and CEO,
Custodiet Advisory
Services



Pravin Kumar
CIO at Wibmo Inc.,
a Naspers/PayU
company



Jörgen Mellberg
CISO & Head of IT,
Sparbanken Syd



David Monahan
SVP, Business
Information Security
Officer, Bank of America
Merrill Lynch



Michael Owens
Business Information
Security Officer, Equifax



Jules Pagna Disso
Group Head of Cyber
Risk Intelligence & Insider
Technology Risk, BNP Paribas

A Challenging Year for Financial Services Cybersecurity

Last year saw an increase in attacks targeting financial firms, as companies scrambled to adapt to new ways of working in the wake of the COVID-19 pandemic

Banks have always been a target for criminals. But in the digital era, the most successful criminals are not cracking safes for cash. They are penetrating firewalls for data.

Even before the pandemic, cybersecurity for financial firms involved high stakes. In addition to the sensitive data they hold, banks and financial institutions also control bank accounts, credit card information and other financial assets.

But COVID-19 caused a surge in attacks on financial institutions. Cloud anti-virus firm VMware Carbon Black found a 238% increase in cyber-attacks on the industry in the 2020 edition of its Modern Bank Heists report.

"Direct access to money and payments is very attractive for attackers," says BNP Paribas Group Head of Cyber Risk Intelligence Jules Pagna Disso.

"Cyber risk is the largest risk now that is facing any organization in the world," adds Voya Financial SVP Global Chief Information Security Officer Raj Badhwar. "It used to be the traditional risks, like the finance risk, the credit risk or the volatility of the market. But now cyber risk has circumvented all those."

A successful breach can cause serious business and reputational damage for financial firms. This has propelled cybersecurity to the top of the agenda for senior leaderships and raised the profile of the CISO in the corporate hierarchy.

238%

The increase in cyber-attacks on financial firms in 2020

Source: VMware 2020

"Direct access to money and payments is very attractive for attackers."

Jules Pagna Disso

Group Head of Cyber Risk Intelligence,
BNP Paribas

How IT Security Leaders Responded to COVID-19

Concerns about cyber risks caused by complex IT infrastructures are hardly new. Research from consulting firm Deloitte shows that the issue has been a top priority for senior leadership in financial firms in each of the last three years.

However, cybersecurity executives had to make rapid changes to company IT infrastructures in response to the pandemic, expanding virtual private networks and implementing multi-factor capabilities to ensure end-to-end security.

Executives are acutely aware that mistakes during this transition to business models that enable remote working may compound network complexity, increase the 'surface area' that attackers can target and create vulnerabilities that bad actors will be keen to exploit.

"If you have a large attack surface, you will definitely struggle to keep up with the attackers, because they are so diverse," warns Pagna Disso.

For many cybersecurity executives, responding to targeted attacks on users in their own homes meant a new focus on raising employee awareness about phishing attacks and the importance of using protected systems and tools properly.

"Working from home for a long time is very different, not least from a technical perspective," says Zsuzsanna Berenyi, Cyber Security Awareness and Culture Expert at London Stock Exchange Group "You have to be continuously making sure that even your home devices are secure and your home network is secure."

Jörgen Mellberg, CISO and Head of IT at Swedish bank Sparbanken Syd adds: "It might be tempting when you're working from home to just take that USB key and move over your data to a home computer to be more efficient. But this could be a breach both to policies and regulations such as the [Bank Secrecy Act](#)."

Ensuring IT infrastructures remain compliant with global cybersecurity regulations has also proved challenging in

the age of COVID-19.

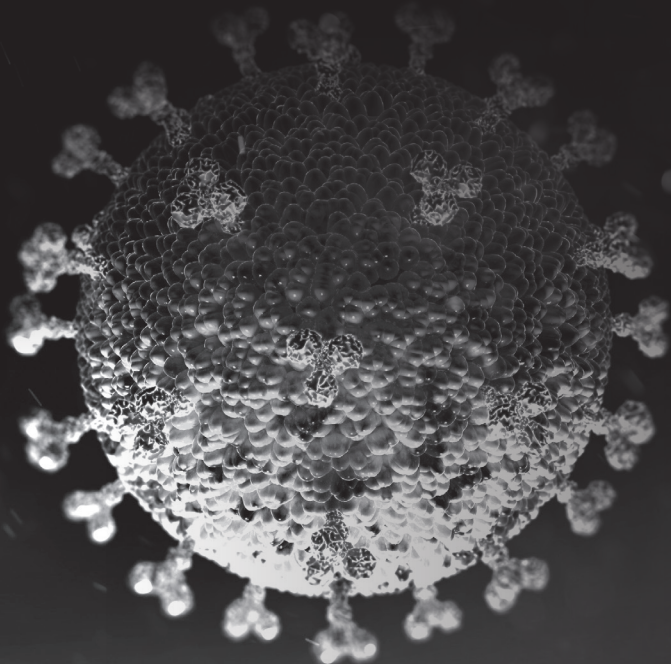
"We have multiple data centers across the world. Ensuring that all of those locations met all of our security requirements for remote access was paramount," says Bank of America Merrill Lynch SVP Business Information Security Officer David Monahan. "Initially many of the locations weren't designed for remote access, so the main impact was ensuring that we had a uniform security methodology across our global footprint."

He adds: "We're responsible for our banking compliance requirements, regardless of what is happening in the external world. The big thing is making sure we have reviewed the architectures and the deployments to ensure that we were going to be compliant."

"Initially, many of the locations weren't designed for remote access. So, the main impact was ensuring that we had a uniform security methodology across our global footprint"

David Monahan

SVP Business Information Security Officer,
Bank of America Merrill Lynch



Cloud Migration is Creating New Cybersecurity Priorities

Innovation at the cutting edge of technology is the key to survival in a competitive marketplace. However, new technology alters traditional network boundaries and may create additional risk.

Cloud technology and the explosion of 'software as a service' has enabled financial firms to increase their business agility, experiment with new technology and reduce capital expenditure. As a result, CTOs increasingly want to move applications and infrastructure to the cloud.

This industry shift is raising concerns for some cybersecurity executives. But others now feel that these concerns can be addressed.

"CISOs in the financial services are worried about our exposure, as we have rapid migration of our systems and services to the cloud," says Voya Financial SVP Global Chief Information Security Officer Raj Badhwar. "The problem is that sometimes security gets neglected a little bit."

"Services that were done in-house are now being moved to the cloud," adds Equifax Business Information Security Officer Michael Owens. "That in itself redefines what your network boundaries look like and how you handle endpoint security."

When Capital One's cloud infrastructure was breached in 2019, the hacker's activity went undetected for months. This example highlights the importance of visibility to the timely detection of data theft. Achieving this relies on the kind of basic monitoring that can be easily overlooked.

"The most fundamental security control after perimeter is basic monitoring and visibility," says Badhwar. "If you are rapidly migrating your business to the cloud, you have got to have your perimeter controls figured out. And then the most important thing is your monitoring and detective controls."

"Cloud is actually very secure if you do it properly," he concludes. "Whether it is AWS, Azure, Oracle or Google, they all have the capabilities and security controls required that were there in the traditional data centers." ■

"CISOs in the financial services are worried about our exposure as we have rapid migration of our systems and services to the cloud. The problem is that sometimes security gets neglected a little bit"

Raj Badhwar

SVP, Global Chief Information Security Officer, Voya Financial



SolarWinds: Key Learnings from an Unprecedented Breach

The latest posterchild of third-party risk raises serious questions for cybersecurity executives about the assessment and oversight of technology vendors

Network monitoring software firm SolarWinds was notified of a major supply chain hack of their Orion Platform using malware known as SUPERNova on December 12, 2020. Attackers weaponized platform updates to spread the SUPERNova malware to SolarWinds' network of customers.

Ultimately, the hack may have affected up to 18,000 companies and government agencies in the US. Widely thought to be the result of Russian state-sponsored cyber espionage, the true perpetrators are still unknown, as are the true scale of and motivations for this unprecedented breach.

"Everyone knew it was possible," says Sparbanken Syd CISO and Head of IT Jörgen Mellberg. "But that it would blow up like this with such a big vendor as SolarWinds with enterprise systems that almost everyone is using? That was really an eye-opener."

The breach eluded world-class cybersecurity teams at some of the US' largest companies for months, and went as far as compromising Microsoft's cloud protections, allowing the hackers to access its source code.

For cybersecurity executives, the hack raises questions about network vulnerability because of supply chain hacks from third-party vendors.

Mellberg concludes: "You really need step-by-step processes of how to assess your third parties and how they handle your risks and potential incidents like this."

18,000

the number of companies potentially affected by the SolarWinds hack

Source: SEC, 2020

"Everyone knew it was possible. But that it would blow up like this with such a big vendor as SolarWinds with enterprise systems that almost everyone is using? That was really an eye-opener"

Jörgen Mellberg

CISO and Head of IT, Sparbanken Syd

Evaluating Third-Party Vendors on Risk

One reason the SolarWinds hack is so concerning for corporate cybersecurity experts is that compromised updates from third parties are so hard to detect.

Patching and updating software is itself one of the most basic protections against cybercrime. But what if those patches and updates, seemingly authentically signed, are introducing malware to your network?

"We all use a lot of third parties, and there is no way that each and every integration and each and every package, upgrade or update can be scanned," says Voya Financial SVP, Global Chief Information Security Officer Raj Badhwar. "There is no way that we can detect using traditional means all the malware that may be hidden in there."

For many cybersecurity executives, this has meant a new focus on evaluating third-party technology providers based on their cybersecurity credentials. However, there is no regulatory guidance on how this should be done, leaving negotiations to be conducted largely on a case-by-case basis.

"Unfortunately, there's no regulation to force a third-party's hand on compliance,"

notes BNP Paribas Group Head of Cyber Risk Intelligence Jules Pagna Disso. "You might point out during that [they] have a number of vulnerabilities that we feel can be exploited. It works for some, but it doesn't always work for others."

Technology solutions such as BitSight or RiskRecon can help with this process, of course. But you don't need a multi-million-dollar program to get started. The process begins with the basics of global sourcing and vendor management.

"If you don't have anything in place, then ensure that you build out a questionnaire containing basic security information," advises Equifax Business Information Security Officer Michael Owens. "Get [vendors] to fill it out. Start to capture some basic information and build out a tracking program."

"If you do have a program, then it really has to be about refining it," he adds.

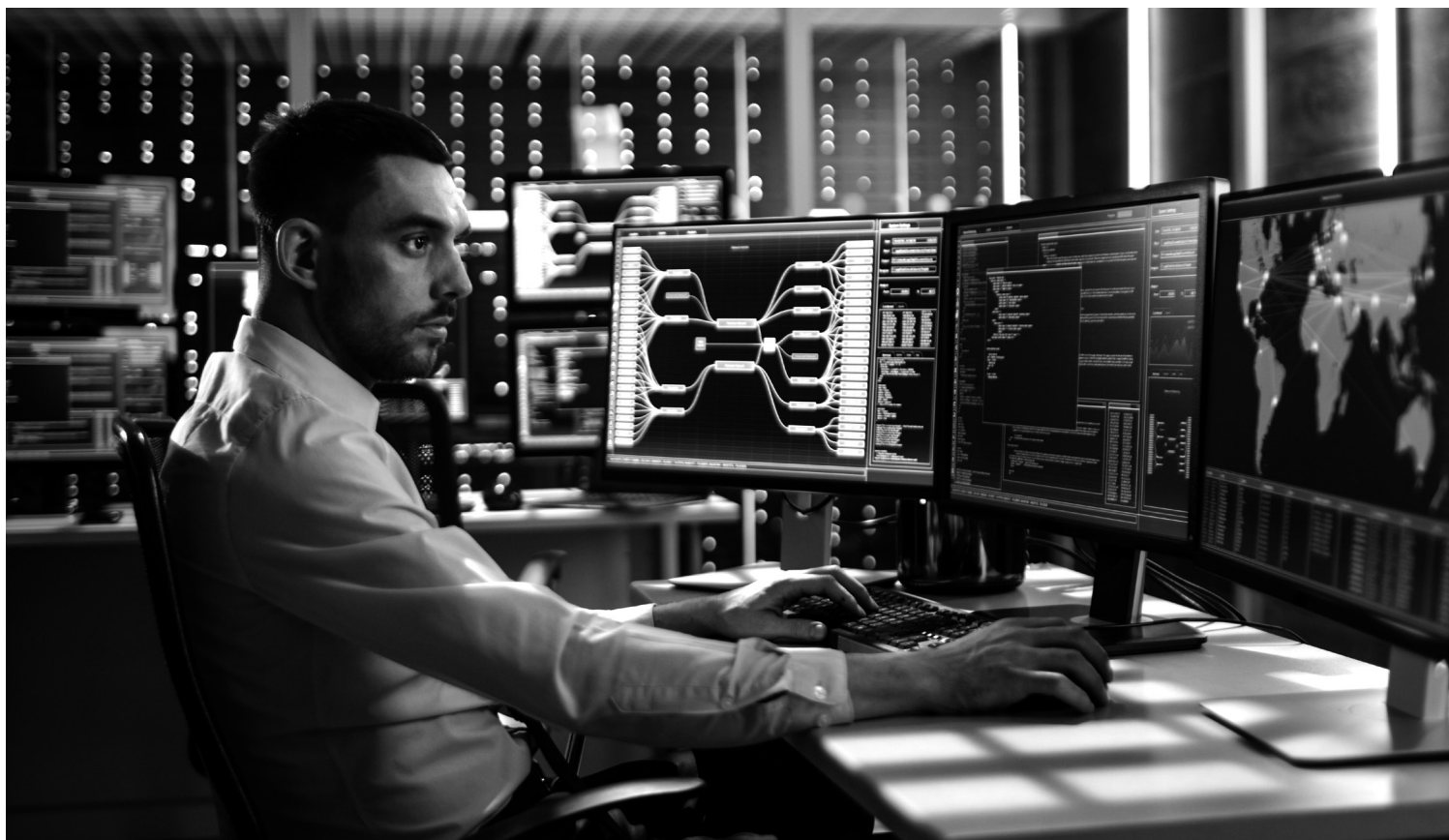
"Working to mature that program and ensure that the visibility is raised to the point where information security is really baked into that process."

"Every company is a target, and it doesn't matter what business or what industry you're in," he concludes. "Attackers are constantly and consistently going to find ways to try to infiltrate your environment."

"It doesn't matter what business or what industry you're in. Attackers are constantly and consistently going to find ways to try to infiltrate your environment"

Michael Owens

Business Information Security Officer,
Equifax



Locking Down Lateral Movement to Reduce Exposure

While risk can be mitigated with careful vetting of technology vendors, the possibility of a breach introduced by third-party software can never be eliminated.

"It's not about that if we will be attacked, it's about when we will be attacked," warns Pravin Kumar, CIO at payments company Wimbo. "In parallel, it is also true that you can be safe and secure to some extent as well. It's not rocket science. But it's important to create basic technology hygiene."

Technology hygiene starts with threat detection and careful use of account management to limit the ability of a bad actor to move laterally across the network, Kumar explains.

"It's crucial to look for lateral movement in attacks that are going on and evaluate technologies that can watch for individuals trying to either access systems or data inappropriately," says Bank of America Merrill Lynch SVP Business Information Security Officer David Monahan.

"It's important to firewall, and essentially isolate authorized communications between applications to restrict unauthorized entities from accessing those applications while trying to move laterally or exfiltrate data," he concludes.

This example highlights the importance of account management to ensure that users, human or computer, only have access to the parts of the network that are necessary. This is especially true of accounts with administrator privileges which are the biggest prize for any would-be attacker.

Cybersecurity executives focused on preventing the spread of an attack know that the internal security is as important as the external security.

"Administrators should not be allowed to administrate the whole environment, administrative rights should be limited and compartmentalized," says Pagna Disso. "Unfortunately, many businesses do not take their internal vulnerabilities as seriously as the ones that they expose to the internet." ■

"It's important to firewall, and essentially isolate authorized communications between applications to restrict unauthorized entities from accessing those applications while trying to move laterally or exfiltrate data"

David Monahan

SVP, Business Information Security Officer, Bank of America Merrill Lynch



Mitigating the Danger of Insider Threats in Financial Institutions

Cybersecurity executives are implementing measures to control the damage that can be caused by bad actors who already have a foothold inside networks



The threat insiders pose to data integrity and security is a growing concern for many cybersecurity executives in financial firms. A 2020 report from cybersecurity company Gurukul [reveals](#) that 68% of organizations feel vulnerable to insider threats.

However, while the term ‘insider threat’ is commonly used to refer to employees misusing their credentials to steal data or inappropriately access systems, it can have other meanings.

For example, a mistake by a well-meaning employee can leave the door open to bad actors, enabling them to gain access to the network by hijacking an unsuspecting user’s account. This kind of accidental incident may even be more common than malicious data theft.

In [a study](#) by cybersecurity software provider Netwrix, 59% of financial firms said employees sharing data accidentally

or administrators making mistakes had caused cybersecurity incidents. Just 11% had experienced data theft.

It is crucial for cybersecurity executives to distinguish between accidental and malicious behavior in their organizations. This affects both how the incident should be addressed and wider perceptions of the cybersecurity team.

“We’re not here to be big brother in a sense that we’re trying to find a way to crucify you,” quips Bank of America Merrill Lynch SVP Business Information Security Officer David Monahan. “It’s all about separating that insider threat from the threat on the inside.”

He adds: “We may need to discipline [staff] from either an ignorance or misbehavior perspective. For clicking on the link, but not from the perspective of someone who is one trying to steal our data.”

59%



is the number of financial firms who reported a cybersecurity incidents due to accidental data sharing by employees or mistakes made by administrators

Source: Netwrix, 2020

The Evolving Threat of Social Engineering

Cyberattacks are rife in the age of COVID-19. Research from email security firm GreatHorn shows that 53% of cybersecurity professionals have seen an increase in email phishing attacks during the pandemic.

“We saw a huge number of attacks [because of the pandemic],” says BNP Paribas Group Head of Cyber Risk Intelligence Jules Pagna Disso. “But rather than being directed at the business, what we have observed is that the attacks were directed at end-users.”

Of course, phishing attacks have been around for a long time. What is new is the intricacy and personalized nature of the attacks, in many cases rising to the level of ‘social engineering’.

The ‘social engineer’ uses psychological manipulation to trick people into giving up personal information, or otherwise compromising their security. During the pandemic, attackers used these techniques to target employees working remotely, capitalizing on fear and uncertainty.

“Most of the attacks that we have seen have been around the COVID-19 theme,” says Pagna Disso. “When targeting people directly in their personal environment, people have a certain fear that they will not necessarily disclose to their employer, and the attackers were trying to take advantage of that.”

“Social engineering is the single largest attack surface that we have, because it’s one of the most effective,” notes Equifax Business Information Security Officer Michael Owens. “It goes beyond just phishing or spear phishing. It targets human

behavioral elements in the attack, which makes it so effective.

To fight this evolving threat, cybersecurity executives are renewing their approach to training and awareness. They are focused on raising awareness about how to recognize phishing or social engineering attacks and how easy it can be to fall for sophisticated ones.

“Awareness is very important,” concludes Pagna Disso. “In the corporate environment you probably expect [the threat] to be presented a certain way. But when working from home, they might not know what to expect.” ■

“We saw a huge number of attacks [because of the pandemic], but rather than being directed at the business what we have observed is that the attacks were directed at end users”

Jules Pagna Disso

Group Head of Cyber Risk Intelligence, BNP Paribas



Trust Issues: Adopting a Zero Trust Framework

Adopting a zero-trust infrastructure has become a priority for many cybersecurity leaders as their businesses rapidly expand their data use

Rapid digitalization, the widespread move to a 'work from home' environment and the continued deployment of cloud computing has expanded networks and highlighted the importance of robust internal security postures.

The zero-trust architecture model was first created in 2010. But it has moved into the mainstream recently, partly due to rapid increases in the amount of vital business data held in enterprise systems and the increased sophistication of cyber attackers.

As a concept, zero trust pushes back against the idea that anything inside of the corporate firewall is safe. Instead, it treats every request as if it came from an open network.

"We should not be letting anonymous people or systems in [to our networks], information should not be left in a native machine-readable format and networks should not be traversable by unvalidated entities," states Steve Jump, Director and CEO at cybersecurity consultancy Custodiet Advisory Services. "None of this is new. Zero trust just puts a spotlight on those principles."

However, zero-trust architecture is not a cybersecurity panacea. Its key technologies – including but not limited to multifactor authentication, identity and access management and next-generation endpoint security – require continuous monitoring and validation to be effective.

"None of this is new. Zero trust just puts a spotlight on those principles"

Steve Jump

Director and CEO, Custodiet Advisory Services



Laying the Foundations for Zero Trust

While there are many commercially available zero trust solutions on the market, it is possible for cybersecurity executives to implement aspects of zero trust using their existing technology stack.

“A fundamental tenant of zero trust is network micro-segmentation,” explains Voya Financial SVP Global Chief Information Security Officer Raj Badhwar. “That you could do, depending on how complex your network is, without a specific tool.”

To achieve this, a cybersecurity leader might break up their company’s network into multiple segments. Then, if a user in a given segment is breached, the attacker can’t move laterally across the network.

From there, a company can control access to network segments using

personas. Each employee persona is granted the minimum network privilege required for them to do their job.

“If [you have] a contractor, then maybe they should only get access to outlook exchange, the timesheets system and two other systems that they’re working on,” Badhwar says. “That’s it.”

Of course, cybersecurity experts should be cautious. Implementing zero-trust architectures is complex, time consuming and requires that detailed logs and entries in configuration management databases are kept up to date.

“[Zero trust] will increase the complexity of implementation and maintenance,” warns Badhwar. “Debugging becomes difficult because of segmentation, and end-to-end encryption means that all traffic is also encrypted, so that creates support problems.”

“[Zero trust] will increase the complexity of implementation and maintenance”

Raj Badhwar

SVP, Global Chief Information Security Officer, Voya Financial

Zero Trust or Minimum Trust?

While few cybersecurity executives would argue about the importance of the principle of least privilege or the need to regularly refresh their registries of active users, zero trust can prompt a mixed response.

For some, this is a reaction to the overuse of the term in aggressive marketing campaigns. Others feel that the nomenclature of zero trust is too absolute, despite its sound principles.

"If you have zero trust, no business gets done," says Bank of America Merrill Lynch SVP Business Information Security Officer David Monahan. "So, it's really about minimum trust."

"But with that in mind, it comes back to principles," he concludes. "What level of access do you need to do your business? We should make sure you have that access and no more. Security is here to facilitate business in a secure manner, not to stop business from happening."

To determine what 'minimum trust' might mean in practice, CISOs may choose to conduct a thorough audit of roles and responsibilities in their organizations to determine appropriate levels of network access.

A [report](#) from consulting firm Deloitte recommends internal auditing to identify vulnerabilities and bolster the third line of defense against cyber-attacks.


As companies continue to digitize and apply more cloud-based applications and services we are likely to see a greater emphasis on the principles that underpin zero trust. However, leading CISOs also know that a focus on zero trust should not undermine cybersecurity's role as a business enabler. ■

"Security is here to facilitate business in a secure manner, not to stop business from happening"

David Monahan

SVP, Business Information Security Officer,
Bank of America Merrill Lynch





Discover More Essential Information Security Insights


As anyone who has attended our global conferences or events will know, our 300,000-strong network of information security leaders boasts many of the most forward-thinking minds in the industry.


Our new content hub, [Business of InfoSec](#), brings those same essential insights direct to you and is packed with exclusive research, video podcasts, in-depth articles, interviews, and reports. Discover how other information security leaders are tackling the challenges they face today while maintaining the confidentiality, integrity, and availability of their organization's data.

For a limited time, subscribing to the [Business of InfoSec](#) is free. So, make sure to subscribe today for complimentary access to exclusive insights you just can't find anywhere else.

SUBSCRIBE NOW

business
of **InfoSec**

 Follow us on LinkedIn

 Follow us on YouTube

About the Editor

Gareth Becker is an experienced editor and content marketer and produces B2B stories that focus on emergent trends in data and analytics, cloud computing, information security and more.

He works with world-leading brands to shine a light on fresh ideas and innovative products using a range of multimedia content.

To share your story or enquire about appearing in a Corinium report, blog post or digital event, contact him directly at gareth.becker@coriniumgroup.com



Gareth Becker
Content Strategist,
Corinium Global Intelligence

Partner with Corinium Digital

We'll develop in-depth benchmarking research, special reports and editorial content to establish your brand as an industry thought leader.

Find out more:

www.corinium-digital.com









Discover Corinium Intelligence

Corinium is the world's largest business community of more than 300,000 data, analytics, customer experience and digital transformation leaders.

We're excited by the incredible pace of innovation and disruption in today's digital landscape. That's why we produce quality content, webinars and events to connect our audience with what's next and help them lead their organisations into this new paradigm.

Find out more: **www.coriniumintelligence.com**

Connect with Corinium

-  **Join us at our events**
-  **Visit our blog**
-  **Read our white papers**
-  **Follow us on LinkedIn**
-  **Follow us on Twitter**
-  **Like us on Facebook**