Supply Chain Security Trends, Australia

2022

Australian cybersecurity leaders discuss challenges in supply chain cybersecurity management and consider best practices for security teams

RAPID7

Corinium

Contents

Click below to navigate

Executive Summary

Supply chains represent a considerable area of risk for organisations all over the world. From software to services, any engagement an organisation has with an outside party comes with risk that must be managed.

With large organisations participating in more supply chains than ever, and those relationships often being deep, the surface area for potential threats grows ever wider, with new conduits for cybercriminals to traverse and attack their targets.

Featuring insights from interviews and independent research, this report explores the way Australian security leaders consider and manage the cybersecurity risks through their chain of suppliers.

Our discussions reveal how cybersecurity leaders think of and categorise risk when it comes to third parties, how they manage this risk through due diligence and continual review, and the major challenges they identify along the journey. ■

Contributors

Jo Stewart-Rattray, Chief Information Security Officer, Silver Chain Group

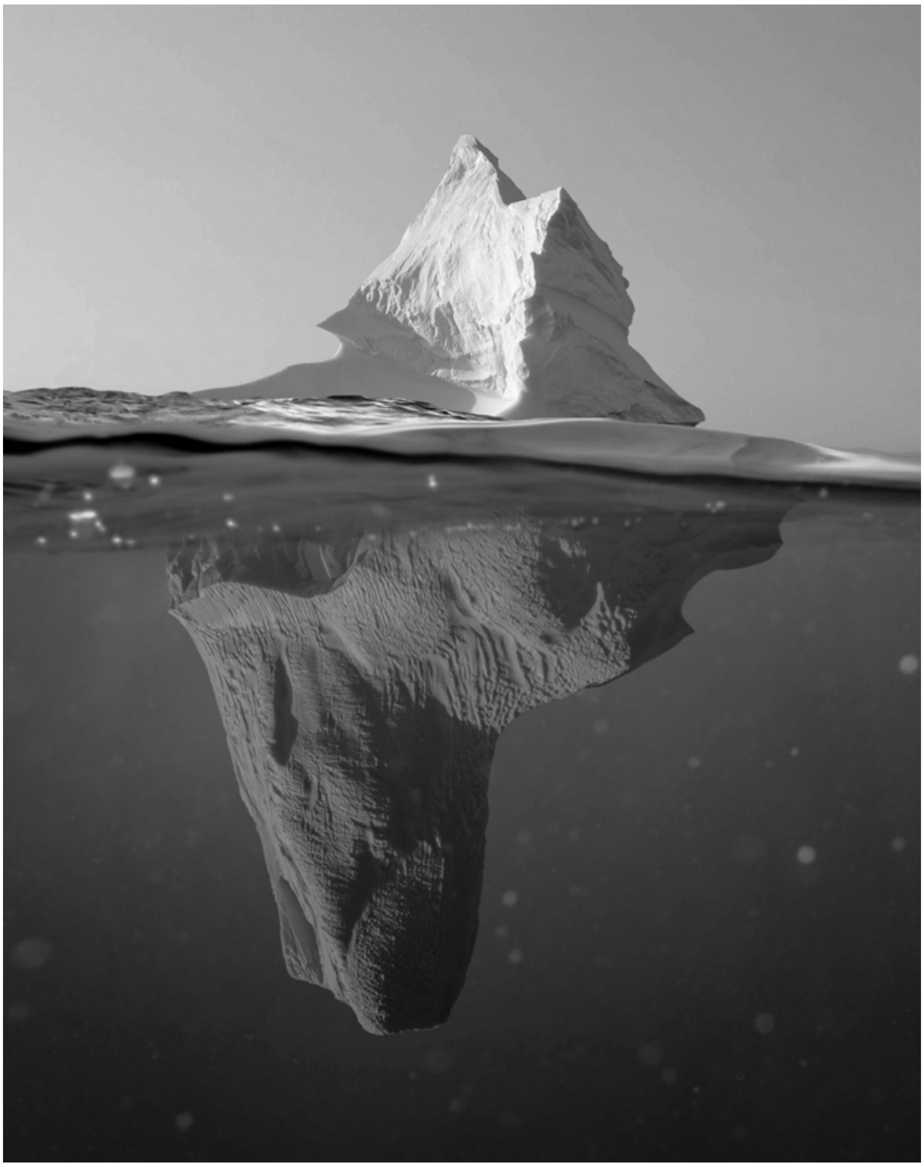
Christoph Strizik, Chief Information Security Officer, Origin Energy

Rob Wiggin, Consultant, Former Chief Information Security Officer, Queensland University of Technology

Robin Long, Regional Manager, APAC- Incident Detection and Response, Rapid7

The Risk in the Supply Chain

Supply chain attacks represent a pressing and relevant modern cybersecurity concern that organisations everywhere must consider



Whether it's accounting software, computer and networking hardware, contracted employees or hired consultants, third-party suppliers can sometimes plug deeply into customer organisations, gaining access to networks, systems and data to ensure highly productive partnerships.

This engagement represents a considerable risk area for cybersecurity leaders to monitor and manage.

The Australian Cyber Security Centre, the Australian Government's lead agency for cybersecurity, has advised that all organisations should consider cyber supply chain risk management.

The agency states that: "If a supplier, manufacturer, distributor or retailer are involved in products or services used by an organisation, there will be a cyber supply chain risk originating from those businesses. Likewise, an organisation will transfer any cyber supply chain risk they hold to their customers."

One of the most recent high-profile supply chain breaches was last year's attack of IT software vendor SolarWinds, in which hackers were able to gain access to the software and from within deploy malicious code to its customers via an update.

It was reported that some 18,000 customers around the world installed the tainted patch, including US Fortune 500 companies and government departments.

2017's NotPetya attack is another notable recent supply chain attack. The European Union Agency for Cybersecurity describes the incident as originating when an accounting software vendor had its infrastructure compromised by a threat actor, who then tampered with the software and pushed a malware-laden version of it out to the vendor's customers as a legitimate update.

In the event of a supply chain security incident, customers of a breached operator can be subject to spying, data theft, ransomware or loss of control of their critical operations. In addition to huge costs to remediate, these breaches can destroy brand reputations and expose the private details of citizens.

The Supply Chain Attack Surface

Part of the reason cybersecurity leaders must be more conscious than ever of supply chain risk has to do with the increasing reliance on technology solutions to operate organisations efficiently and competitively in the modern age.

"Organisations need to focus on their core competencies, so they rely on suppliers and partners to fulfill their broader requirements," says Rapid7 Regional Manager, Incident Detection and Response, APAC, Robin Long.

The market is full of solutions and practitioners pitching to help alleviate administrative, logistical, or technological tasks so business leaders can get on with the core jobs of running their companies.

"There are all of these new partnerships that can be formed to help companies achieve success in the market," Long says.

"The need to remain competitive has organisations relying on a really interconnected world of technologies and suppliers that is driving up the risk to most organisations to these sorts of supply chain attacks."

The more partnering and outsourcing that occurs, the more likely that organisations will witness or even feel the effects of third-party security incidents, Origin Energy Chief Information Security Officer Christoph Strizik says.

"With more and more companies moving to software-as-a-service type offerings, we will continue to see an explosion of third parties within our ecosystem," says Strizik.

"Given that ransomware attacks have drastically increased five-fold over the past 12-18 months, it becomes much more likely that a third-party organisation in the supply chain will suffer an incident that impacts the availability of their services or confidentiality of data, which in turn will adversely impact any organisation that consumes those services.

Jo Stewart-Rattray, who runs a technology and security practice and currently serves as Silver Chain Group's CISO, says another concern for cybersecurity leaders is that there are more IoT and network-connected devices on IT systems than ever before.

"It could be anything from CCTV systems, intercom systems, vaccine fridges, HVAC systems, heating and air conditioning controls. All of those things could either reside on or traverse your network and present a supply chain risk," she says.

> *"With more and more companies moving to software-as-a-service type offerings, we will continue to see an explosion of third parties within our ecosystem"*
>
> **– Christoph Strizik**
> CISO, Origin Energy

The Job of Managing Third Party Suppliers

How cybersecurity leaders conduct supply chain cybersecurity management varies by organisation and supplier type, but there are common considerations cybersecurity leaders should make for each.

"From a security perspective, you really want to know at a minimum what their security culture is and the maturity of their key security controls in place to protect your data and securely deliver the service they offer you," says Origin Energy CISO Christoph Strizik.

"Do they have basic security hygiene (patching and hardening), data protection controls (for example, encryption), sound access management, ability to detect intrusion and ability to respond to an incident? This should be covered in the contract.

"Governance controls are also important. Do they have a security officer? Policies that guide them? Do they align to industry frameworks and practices? Do they do user education and awareness? Do they validate that their controls are working or are there gaps? Vulnerability assessments, independent penetration testing and security attestations play a role here. These are the high-level areas we would explore."

Once due diligence is done, ongoing security assessments must be conducted to ensure security positions do not shift over time.

"The initial risk assessment is only a point-in-time measure, so if in 12 months' time that organisation isn't managing their security controls as well as they were when they were onboarded, you're just as exposed as you would have been without a risk assessment," says Former Queensland University of Technology CISO and cybersecurity consultant Rob Wiggan.

Cybersecurity leaders must also be thinking ahead to when supplier contracts will end, says Origin Energy's Christoph Strizik.

"Can the service provider or vendor delete all of your data from their systems or is that something that will be hard for them to do? Can you easily switch from one provider to another (data migration)? You need to really think about these exit aspects of the relationship upfront," he says.

In the case of consultants or technicians requesting access to an organisation's network, Silver Chain's Jo Stewart-Rattray applies scrutiny.

"If somebody claims they need to be really deeply entrenched at a network-access level, they will have to do the same security checks that my own staff do," she says.

"I'll want to see national police clearance and everything on top of a standard risk assessment. Do they have the credentials? All of that has to be verified. Establish trust and verify." ■

> *"The initial risk assessment is only a point-in-time measure, so if in 12 months' time that organisation isn't managing their security controls as well as they were when they were onboarded, you're just as exposed as you would have been without a risk assessment"*
>
> – **Rob Wiggan**, Former Queensland University of Technology CISO and cybersecurity consultant

Challenges in Managing Supply Chain Security

Complex supplier partnerships, juggernaut vendors and big partner ecosystems throw constant challenges at cybersecurity leaders

Every organisation and every supplier partnership is different, and one of the first challenges cybersecurity leaders must navigate is conducting reasonable risk assessments that demonstrate security alignment between supplier and cybersecurity leader.

The challenge is that not every supplier is going to or be able to place the same emphasis on security, says Rapid7's Robin Long.

"For example, many smaller suppliers might not have the same level of security resources available to them in order to meet your expectations," he says.

Former QUT CISO Rob Wiggan says due diligence often isn't a supplier's favourite job, and there can be some resistance to it.

"Everyone that a third party wants to deal with wants to do the same security risk assessment, so suppliers can get pretty bored of it," Wiggan says.

"I've seen in some cases where they'll only agree to answer your security questions provided you pay them for two days work."

Some suppliers might be so big that they offer standardised security disclaimers that are costly to negotiate.

"If you're dealing with one of the big players, guess what? Sometimes they don't really care much about what you want or need from a risk assurance perspective," says Silver Chain's Jo Stewart-Rattray.

"I've seen a contract from a really large player that essentially said if there was a security breach it isn't their fault and isn't grounds for termination, but of course if we were suspected of having a security lapse we can be cut loose.

"You can end up with your legal counsel battling with their legal counsel to get agreement on security positions. "That's not to say that you can't do that. You can and you should. But it is not without its own cost in both hours and dollars.

"You can end up with your legal counsel battling with their legal counsel to get agreement on security positions"

– Jo Stewart-Rattray, CISO, Silver Chain

"For example, unless you specify it in your agreement, your workloads will not always stay in Australia. You may have something in the Netherlands or the US. When you do demand that all workloads must stay in Australia, you'll often pay a premium."

Cybersecurity leaders need to communicate these negotiation issues with the business and agree on what an acceptable level of risk is going to be when onboarding.

Ongoing Monitoring

A 2019 survey of legal and compliance leaders conducted by Gartner suggested that 73% of the effort that goes into supply chain risk identification is allocated to due diligence and recertification efforts. With only 27% of effort spent identifying risks through ongoing monitoring during a relationship.

Despite this imbalance in effort, 83% of legal and compliance leaders in organisations identified risks in the time after due diligence and before recertification, Gartner reported, and that 31% of those risks resulted in a material impact.

If serious risks can be surfaced through ongoing governance of existing supplier relationships, resources should be allocated to doing that work. However, this is challenging for cybersecurity leaders in organisations with many suppliers.

"If you've got hundreds of suppliers in the ecosystem, do you review them once a year? Unless you are prepared to regularly double your team, that is unsustainable," says Origin Energy CISO Christoph Strizik.

Strizik adds that organisations should dedicate resources to the ongoing monitoring of key supplier partnerships based on the risk category the supplier falls into, particularly if they handle customer data.

In many organisations, however, this categorisation isn't thought through.

"Often this categorisation is driven purely by financial spend," Strizik says. "So, say as an example, anything above $10 million is a tier one and a service contract below $1 million is a tier three. Well in that case, the tier ones get a lot of the attention in terms of due diligence and governance because that's where the money is spent.

"That approach unfortunately isn't really fit for purpose when you think about information security or business resilience risk.

"Maybe you're only spending half a million dollars with a service provider, but if they are getting access to customer details, they probably should be treated as a tier one provider from a risk perspective because if they have a problem, the consequences can be quite significant to the business."

> *"If you've got hundreds of suppliers in the ecosystem, do you review them once a year? Unless you are prepared to regularly double your team, that is unsustainable"*
>
> **– Christoph Strizik**
> CISO, Origin Energy

My Supplier's Supplier

Supplier relationships are not always clear cut. Modern commerce relies on complex and interconnected chains. An organisation may know who its suppliers are, but what about its suppliers' suppliers?

This question poses the challenge of how a cybersecurity leader performs due diligence around a party it doesn't see or isn't aware of.

"I know of one example where the organisation was procuring a service from an industry leader, but all their technical support, data analytics and helpdesk services were outsourced to other providers," former QUT CISO Rob Wiggan says.

"Of most interest is that data analytics part, as this would definitely require access to sensitive data and in this case the underlying storage infrastructure was managed by another party."

In a 2018 survey conducted by the Ponemon Institute, just 15 percent of respondents familiar with outsourcing data risks said their companies knew how their information was being accessed or processed by 'Nth' parties with whom they had no direct relationship. This suggests in the third-party dependant business world we live in today, it can be easy to lose track of who has visibility on your data unless you are being very diligent about it.

"If you have sensitive data such as customer data, personally identifiable information or personnel details, and are sharing that with a third party, you really need to delve further and understand the various other service providers they are using to deliver their service to you," Origin Energy CISO Christoph Strizik says.

"Fourth parties (other third parties used by your supplier) are often neglected during security assessments and this is an oversight that must be avoided.

"You need visibility of the role of these fourth parties and know whether they will be storing and processing your data. If so, you want to know about their security posture too.

"This doesn't mean that you have to assess them as well. You can ask your third party to supply you with the due diligence they have performed. So again, it is always important to understand the particular context and take a balanced risk approach." ■

> *"If you have sensitive data such as customer data, personally identifiable information or personnel details, and are sharing that with a third party, you really need to delve further and understand the various other service providers they are using to deliver their service to you"*
>
> **– Christoph Strizik**
> CISO, Origin Energy

Rethinking Risk

Considerations on planning effective supply chain security programs

We've discussed challenges in due diligence, aligning security profiles, managing, and categorising suppliers based on risk and fourth party issues.

There is no one-size-fits-all security strategy, but planning is key in any cybersecurity program. Having a sense of what to plan for in the assessment and contract phase of a supplier deal can mitigate risk and supplier management dramas before they arise.

"The two elements up front are the initial assessment and what you put in your contract," says Former QUT CISO Rob Wiggan.

"The way we go about doing those assessments is changing though. The first risk assessment and onboarding process I designed I did so at a bank about 10 years ago, we had about 120 ISO2700 questions. If you sent that out to somebody now they would probably tell you to go away.

"You have to distil that down into a smaller number of questions. Think about ones that give you the maximum amount of impact that will drive a further conversation."

When it comes to contracts, these need to offer protection on known and potentially unforeseen circumstances. These might include how a third party will use data, where it will sit, who their third parties are, their liabilities to their customer organisations, termination clauses and how they will communicate a breach.

"You have to put protections in your contracts," Wiggan says. "If you have asked an organisation to do a piece of work, you need to specify that they cannot ask somebody else to do it without your permission, and preferably you would see their risk assessment of that fourth party that will do the work."

Silver Chain CISO Jo Stewart-Rattray says using advisors can definitely help here.

"For certain work, I do use trusted, appropriately experienced and credentialed advisors. Because there are some things you can't keep up to date with in-house, you have to use external help," she says.

"Your processes also have to be reviewed on an annual basis. Because things change over the course of a year, and if your policies don't stay up to date nobody will refer to them."

Stewart-Rattray adds that exit clauses are another key consideration to think of ahead of time.

"In all agreements, there should be a transition-out process that gives assurance that you will get all your data back, that all your instances will be deleted securely, all devices returned, and so on," she says.

"Some of the large vendors will claim that exit processes exist but under a separate contract, at a separate cost, so be wary of that. That's when it's important to ensure that you do have legal counsel involved."

> *"The two elements up front are the initial assessment and what you put in your contract"*
>
> – **Rob Wiggan**, Former Queensland University of Technology CISO and cybersecurity consultant

Vendor Management

As discussed, another big challenge in managing supply chain security is the sheer number of vendors or providers an organisation may deal with. It can be impractical for the cyber team to regularly monitor and audit all third parties, so they must be strategically categorised.

Cybersecurity leaders should help their organisations rethink the way supplier risk is classified in order to dedicate the resources available to constantly monitoring them.

"I would prioritise based on factors like the volume and sensitivity of the data that is shared with the provider or the information assets that they may have access to in order to provide the services," says former QUT CISO Rob Wiggan.

This recategorisation consideration is important as risk has traditionally been based on financial factors, as Origin Energy CISO Christoph Strizik mentions.

"You really have to look at your supply chain and vendor frameworks through a number of lenses, not just the historical commercial/financial one. A key point to consider is the type and value of the information assets as well as the criticality of the service provider," he says.

"This approach allows you to tier or categorise your suppliers in a more holistic and considered way. That is one of the big pitfalls I see with organisations not doing that.

"Scale is also a big issue. As organisations continue to race to the cloud and consume more SaaS, they will have more suppliers in their business processes and it is impossible to review all of them all the time. Having a commensurate assessment approach for each tier is helpful in addressing the scale issue.

"I think some technology solutions that help cybersecurity leaders monitor the supplier landscape or review the security of a supplier can really help you scale up and augment your assurance processes."

In some organisations it may be necessary to rethink the supplier ecosystem from the ground up. Silver Chain's Jo-Stewart Rattray recommends a vendor review.

"Where possible you need to limit the number of vendors you are using," she says. "Why use 51 when you can get away with using 15?
"A lot of organisations have taken an approach that has landed them with loads of vendors.

"That is just more management overhead and security overhead that you really don't need. I've tried to consolidate vendors. When I came into Silver Chain, I did a capability assessment on the security platforms that we use.

"I was looking for any overlap or anywhere there were holes. Part of that was then to look at consolidation of vendors, in some cases where I could have been using one channel partner, I may have been using three. So I consolidated that based on reputation and offering."

> *"Where possible you need to limit the number of vendors you are using. Why use 51 when you can get away with using 15? A lot of organisations have taken an approach that has landed them with loads of vendors"*
>
> **– Jo Stewart-Rattray**
> CISO, Silver Chain

How Much Access do They Need?

It isn't always obvious that suppliers may not need as much access to the systems as they are provided.

Organisations come to trust their suppliers. When a trusted supplier says a patch or an upgrade is required, or an IT consultant wants network access to troubleshoot an issue, the instinct of business has not always been to question.

But this might be changing, according to former QUT CISO Rob Wiggan.

"Sometimes providers say they need administrative access to your server. And you must ask why. You need to think about the process and the piece of work you want them to do," he says.

"Often the business doesn't understand that piece. They say, 'My provider has told me to get this upgraded, they need all this access, let's give it to them'. So, the challenge for security teams is to say, 'No, they don't need all that access, they need only this much'.

"You have to look at your architecture to see if you can support that. Which is kind of where Zero Trust comes in. When you have a particular third party put on this one part of your network, you give them access to the host that they need access to and not your whole server farm.

"It's really about being prepared to be a bit more granular with access. And I'm not sure that everybody understands that yet."

When it comes to services, Silver Chain CISO Jo Stewart-Rattray prefers to take instruction from the supplier and handle the work in-house as much as possible.

"If a vendor says they need to do something in your system. Why do *they* need to do it?" she says.

"Why not do a screen share session with one of your staff members who is already trusted and vetted? That's my preferred method and it affords skills and knowledge transfer too."

Develop Supplier Solutions and Consider Your Own Link

Origin Energy CISO Christoph Strizik says organisations should consider mapping access types and develop solutions specific to supplier types ahead of a supplier engagement.

“We work with many consultants, and we give them a way to access our data safely,” he says.

“There are different technology solutions, such as virtual applications, virtual desktops and others that we apply for different types of business scenarios to enable the required work but limit the level of access to only what is needed to minimise risk.”

When it comes to dealing with suppliers of suppliers, Strizik adds that in addition to putting clauses in contracts with third parties, a lot of data sharing can be de-risked.

“You can de-risk a lot of things by thinking about what data is actually needed and withholding the rest. Can it be de-identified and minimised in any way before being shared? With less valuable data, you have less to worry about when it comes to fourth parties,” he says.

“That’s a good mechanism to reduce the risk profile for your organisation but also helps you to reduce the burden of ongoing assurance and all of those things as well.”

Supply chain security considerations must also include how cybersecurity leaders manage and demonstrate their own security as a potential supplier of services or products to others, says Rapid7 Regional Manager, Incident Detection and Response, APAC, Robin Long.

“There are a number of best practices that can be adopted to ensure a cybersecurity leader minimises the risk of being compromised, to make sure that your part of the supply chain is as secure as it can be,” says Long.

“For example, implementing things like secure code or secure product development practices. Investing in the right balance of secure technologies to both prevent and detect attacks, and of course, making sure that you have access to the right security skills and expertise to help mitigate against the risk of compromise.”

Secure code practices are particularly important from a supply chain security perspective, Long says, as they can mitigate the proliferation of vulnerabilities to reach third parties downstream by guarding against the accidental, or even deliberate, introduction of bugs, defect and logic flaws in production code.

“Then also, depending on the industry that you’re in there are various standards and certifications that your organisation can comply with, like adherence to GDPR, or PCI DSS or SOC2 that basically provide your customers with a level of assurance that you are series about your security practices.”

“You can de-risk a lot of things by thinking about what data is actually needed and withholding the rest”

– **Christoph Strizik**
CISO, Origin Energy

Conclusion

Supply security can be a complex and sprawling area to manage. Cybersecurity leaders should take a 'cradle to the grave' approach, applying governance for the entire lifecycle of a supplier relationship.

Challenges will arise in any supply chain relationship with respect to managing risk, but cybersecurity leaders that understand the importance of good due diligence, detailed contracts and ongoing auditing, in addition to using tools and services to effectively resource these tasks, will be well positioned to succeed. ■

About Rapid7

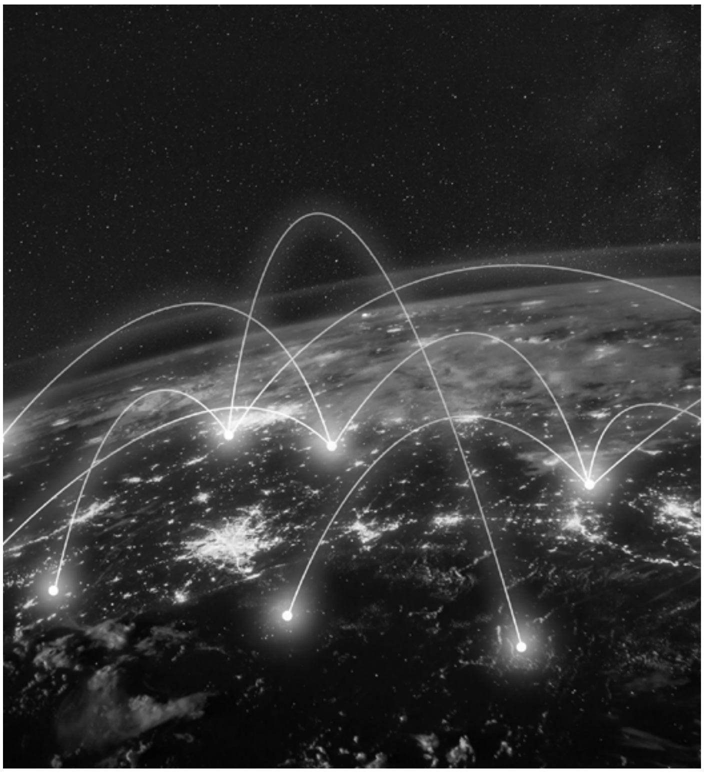
Rapid7 simplifies cybersecurity.

With powerful automation and integrated threat intelligence from our industry-leading researchers and SOC analysts, our Insight Platform gives security teams the visibility they need to secure their environment no matter the size or complexity.

Don't just protect your business, drive it forward.

RAPID7

Find out more: https://www.rapid7.com/



About the Editor

Michael Jenkin is an editor and journalist with more than a decade of experience producing content across broadcast, print and digital media. He specialises in enterprise IT and technology writing.

At Corinium, Michael develops content to inform and support data and analytics and information security executives.

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

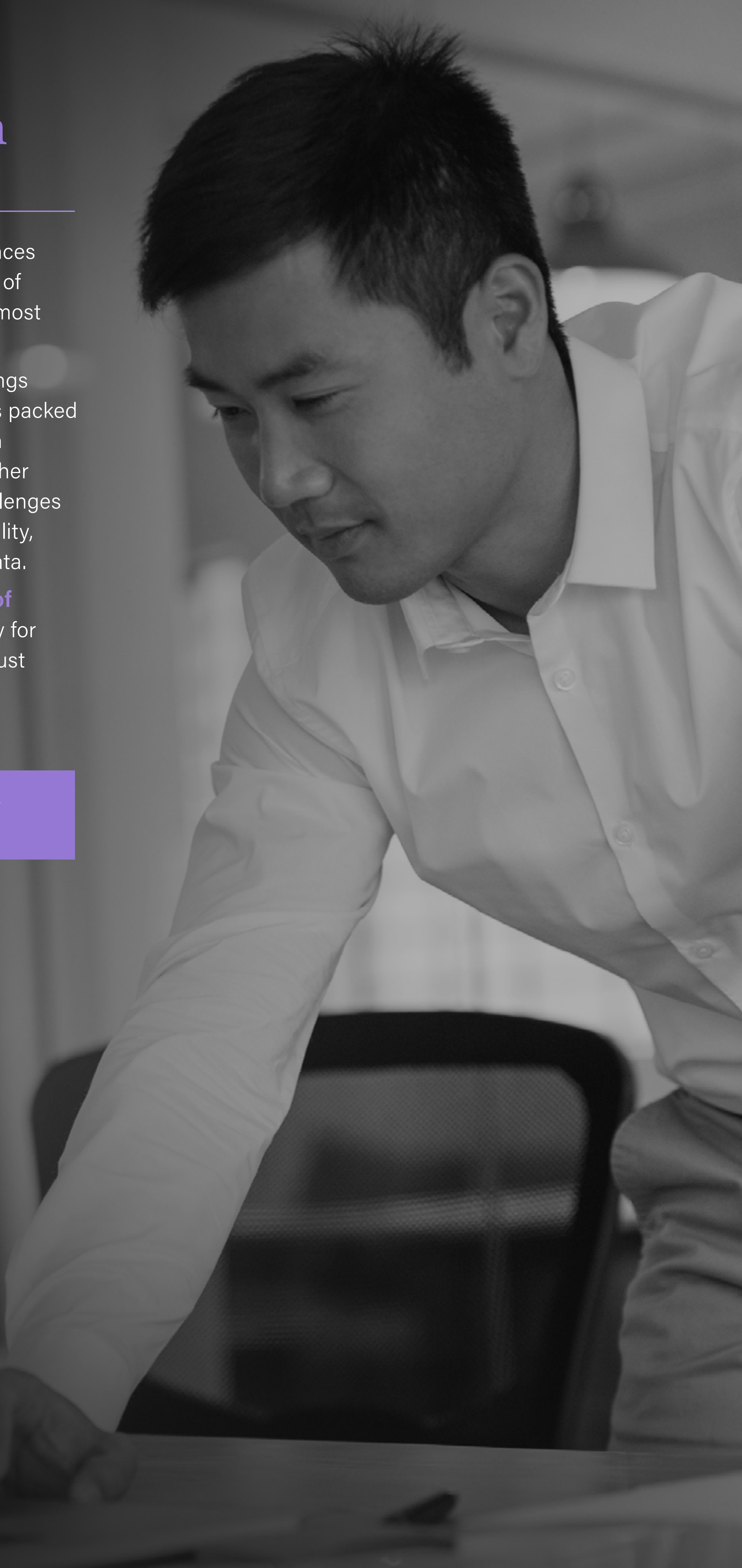
Discover More Essential Information Security Insights

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



Corinium

Partner with Business of InfoSec by Corinium

We'll develop industry benchmarking research, special reports, editorial content, online events and virtual summits to establish your brand as an industry thought leader.

FIND OUT MORE HERE

2021 Global Top 100 Leaders in Information Security

Highlighting the Achievements of Corinium's Global Network of Information Security Leaders

business of InfoSec Corinium

Financial Services InfoSec Trends 2021

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

business of InfoSec Corinium

The 2021 Information Security Agenda

How CISOs Will Navigate Heightened Security Threats in the Wake of the Pandemic and Create Business Value in 2021

business of InfoSec Corinium

Discover Corinium Intelligence

Corinium is the world's largest business community of more than 700,000 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 **reports**
- Follow us on **LinkedIn**
- Like us on **Facebook**
- Find us on **Spotify**
- Find us on **YouTube**
- Find us on **iTunes**