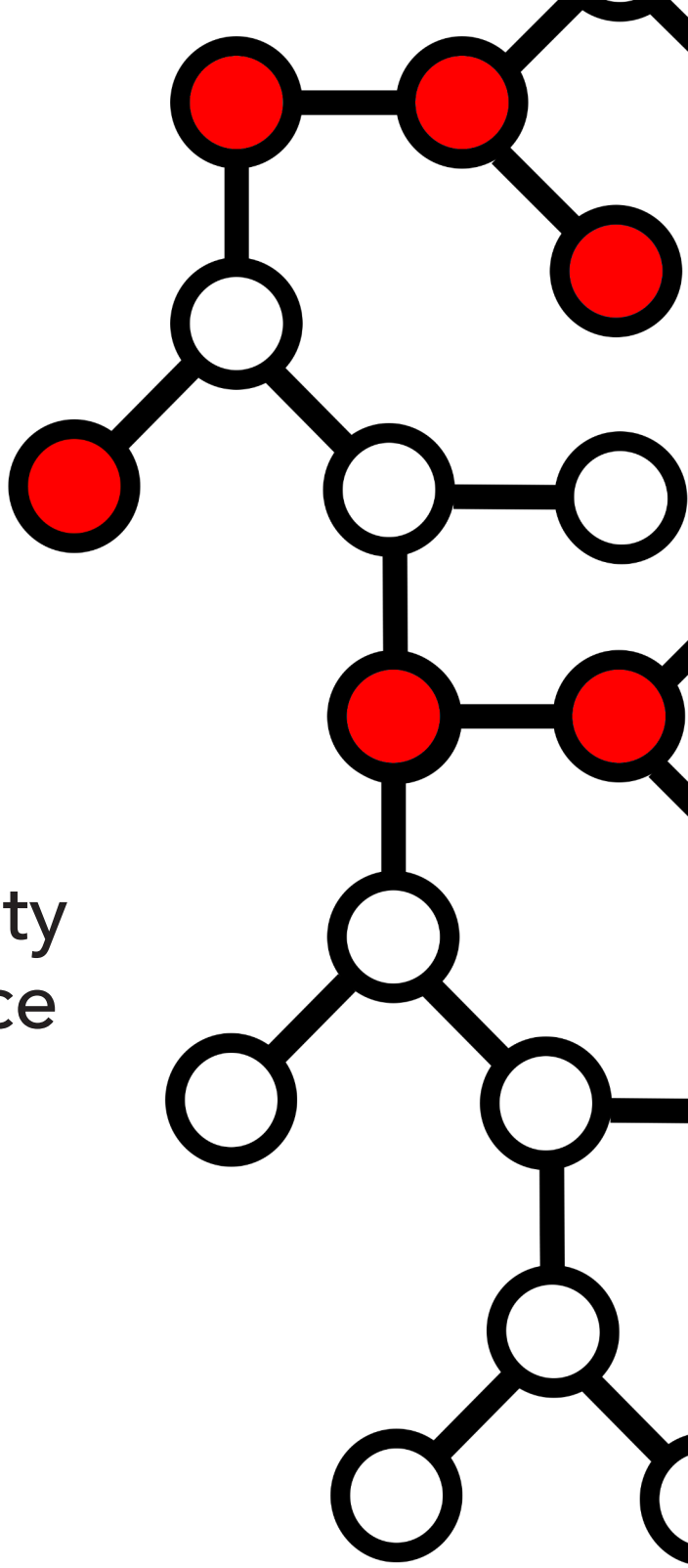


A Guide to Supply Chain Security & Financial Resilience during the COVID-19 crisis

MAY 2020

RISK LEDGER

www.riskledger.com

Introduction

Over 60% of today's data breaches can be attributed to a third party, a number that continues to rise year on year as companies trust an increasing number of suppliers with sensitive and confidential data[1].

A number of high-profile supply chain data breaches have highlighted the impact such attacks can have, and supply chain risk has featured heavily in a number of recent regulations including the EU's GDPR and NIS Directive, California's CCPA and the NYDFS Cybersecurity regulation.

This regulatory environment combined with the potential financial and reputational impact of a supply chain security breach has brought supply chain risk management to the fore. It has risen to become an integral process for any business that relies on its suppliers to process data or provide critical services.

The COVID-19 crisis and associated global lockdowns are causing dramatic increases in the short-term and medium-term risks radiating from an organisation's supply chain.

This paper will examine why supply chain security risk is increasing during the COVID-19 crisis, and why, as a result, supply chain financial risk will increase in the medium-term. It will then go on to explore how organisations can protect and mitigate against this elevated risk and how they should communicate their exposure to the board.

Should you be concerned about your organisation's supply chain?

The short answer is yes. If an organisation transfers data, gives network access, or otherwise gives data visibility to any suppliers, then data protection laws in the relevant jurisdiction and competent business risk management oblige you to manage supply chain risks like any other. Similarly, if an organisation relies on any critical suppliers to be able to operate, developing a comprehensive understanding of their resilience isn't just prudent; it is essential.

There are few organisations who cannot say yes to at least one of those conditions and so it is clear that a macro shock like the current COVID-19 crisis could have a huge impact on an organisation via the supply chain. This is precisely why so many recent regulations draw particular focus to supply chain risk. The price of failing to adequately mitigate this risk could be a fine equivalent to 4% of global turnover in the context of the EU's GDPR[2], and the regulation sets out explicit obligations for organisations to manage the risk of handing data over to third party data processors. In the event of a data breach or operational disruption related to a supply chain failure, organisations also face the cost of their response and recovery, not to mention the possible reputational damage.

If you are unsure of the answer to either of the conditions above, then you are currently in the dark about your exposure to a potentially critical risk to your business. This leaves your organisation on the backfoot compared to your competitors when issues arise in your supply chain during the current volatile business environment.

Detailed analysis of the **2018 Ticketmaster supply chain breach**, by RiskIQ.

The average cost of a data breach in 2019 was

$3.92 million

Could your critical supplier survive this?

IBM, 2019 Cost of a Data Breach Report

Cybersecurity, COVID-19, and your Supply Chain

Since the start of the pandemic, there has been a rapid growth in the attack surface of many organisations as they move to a remote working model driven by government-imposed lockdowns. This larger attack surface inherently increases the risk of successful cyberattacks. However, the speed of the switch to remote working also raises concerns over the quality of security controls implemented to mitigate the risks of this newly remote workforce.

Many companies have had to build and configure new systems quite literally overnight, including the setup of VPNs and multi-factor authentication. Any device used by employees to connect to enterprise networks are now a part of that organisation's attack surface. While VPNs only secure the communication channel between a remote worker's device and the corporate network; they do not protect against malicious activity originating on the device. If a company allows poorly protected, multi-purpose, personal devices to connect to their network, this could be a major threat. Data shows that since the start of lockdowns, use of VPNs has increased by 165% globally and at much higher rates in countries with the most stringent lockdown policies[5]. If attackers compromise a home device and steal VPN credentials, the potential for damage is immense.

In addition to the growing attack surface of most organisations, attackers themselves have updated their tactics to capitalise on the fear and uncertainty that the COVID-19 crisis is causing. This fear is being exploited and used to fuel new social engineering campaigns that have a higher hit rate than they would otherwise have.

Although it is not clear whether the overall volume of

Chris, IT Director at a mid-market accountancy firm in the UK, ran a phishing simulation against staff after implementing remote working for all 580 staff.

"

*Our simulated phishing attack achieved a **10%** click through rate.*

An attacker only needs to succeed once to cause tremendous damage.

Security Threat Resources during the COVID-19 Crisis

List of cyber-attacks and threats related to COVID-19 collated and maintained by **WebARX**.

List of COVID-19 related indicators of compromise (IOCs) maintained by **Sophos**.

List of mitigation advice for COVID-19 related cyber threats maintained by the US **Department for Homeland Security** (DHS), **Cybersecurity and Infrastructure Security Agency** (CISA) and the UK's **National Cyber Security Centre** (NCSC).

Detailed analysis of recent COVID-19 related ransomware and 'infostealer' attacks maintained by **Unit 42 of Palo Alto Networks**.

threats has increased, it is the increase in their success rate that is contributing to the growing security risk of a supply chain breach. Microsoft has shared threat intelligence showing that "*every country in the world has seen at least one COVID-19 themed attack…and that the volume of successful attacks in outbreak-hit countries is increasing, as fear and the desire for information grows.*"[4]

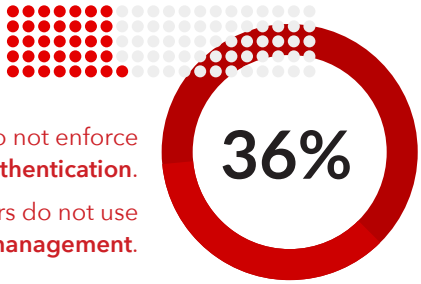
The combination of these two forces - the increasing rate of successful cyberattacks[3] and the increased attack surface of most organisations - will lead to an increase in the number of successful data breaches over the next few months. Data suggests that small and medium-sized enterprises will be hit the hardest[6] by this wave of attacks due to lower security budgets, but larger organisations with established security teams will also feel the impact of this through their supply chains.

The Risk Ledger platform enables organisations to run a gold standard risk assurance programme against their supply chain using our standardised Supplier Assessment Framework (SAF) developed with support from the UK's National Cyber Security Centre (NCSC). The SAF is a comprehensive, standardised, assessment of a supplier's security posture covering a range of security domains. Once completed, suppliers can share their assessment with multiple clients at the click of a button in a 'do once, use many' assessment model.

Insights from the security assessments of suppliers on the Risk Ledger platform (completed before suppliers take advantage of the free support Risk Ledger offers to improve supplier security controls) paint a worrying picture about the security resilience of supply chains. 36% of suppliers do not enforce multi-factor authentication on remotely accessible services and the same percentage do not secure the use of business mobile phones using mobile device management (MDM). Given the increased risk of cyberattacks, lack of preparedness by suppliers is also cause for concern. 15% of suppliers lack a business continuity plan and do not provide information security training to their

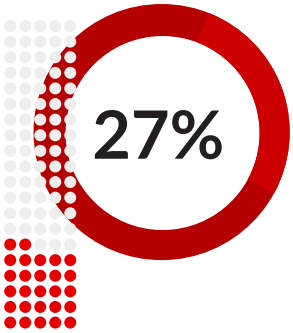
employees, whilst over 10% of suppliers do not have a documented incident response plan[5].

If your organisation shares any confidential or sensitive data with its suppliers, or gives network or data access to them, this will be a key risk over the coming year.

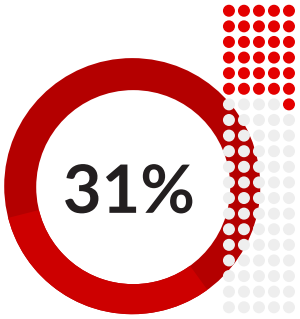


36% of suppliers do not enforce **multi-factor authentication**.

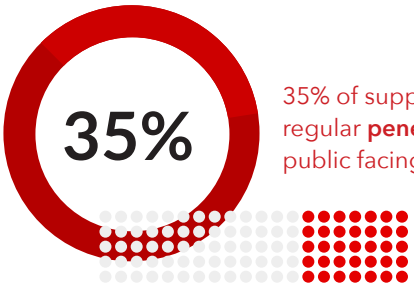
36% of suppliers do not use **mobile device management**.



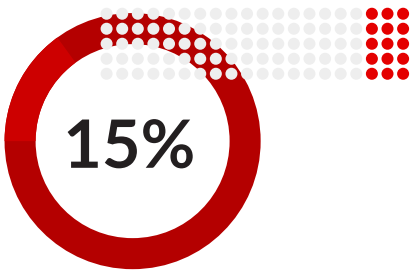
27% of suppliers do not have formal agreements to control third-party use of data that include **GDPR requirements**.



31% of suppliers have not implemented **network monitoring controls** such as IDS, IPS or SIEM systems.



35% of suppliers do not conduct regular **penetration tests** of their public facing IT infrastructure.



15% of suppliers do not provide **information security training** to their employees.

Financial Stability, COVID-19, and your Supply Chain

COVID-19 is causing vast uncertainty in the financial markets, and lockdowns are pushing entire sectors into financial distress. A global recession is now predicted and with markets around the world still reacting to the COVID-19 crisis, many economists even believe that while a recession is highly likely, a depression is a distinct possibility[6].

Despite the unprecedented measures taken by governments and central banks to limit the economic impact of the crisis, this hostile trading environment is already creating tough financial challenges for many businesses and will continue to do so as the short-term, lockdown disruption turns into medium-term economic tumult. Sharp contractions in demand will cause cash flow problems, reduced access to loan facilities and expose unsustainably high fixed costs.

In 2009, as the effects of the credit crisis recession kicked in, the rate of business 'deaths' increased by 23% compared to the year before in the UK[9]. Even more worrying for the supply chain is the data for specific business sectors. In that same year, the number of business 'deaths' in the UK information technology and computer programming sector increased by 46% compared to the year before and by 2010, the equivalent figure in the auxiliary financial services sector, which includes financial transaction processing (but excludes businesses involved in banking, insurance and pensions), was a staggering 74%[9].

If similar trends are observed in the medium-term due to the COVID-19 response, you should expect huge disruption within supply chains, reminiscent of the disruption caused in the aftermath of the 2008 financial crisis[8]. For organisations who rely on critical suppliers to maintain the delivery of their own services, this will be a key risk over the next two years.

In addition, insights drawn from the Risk Ledger platform suggest that over 30% of suppliers do not have a cyber insurance policy in place[5], highlighting the fact that both security and financial risks are closely entwined – an increase in cyber-attacks will lead to an increase in financial failures within your supply chain as companies bear the high cost of reacting to data breaches.

In 2009, during the financial crisis, business deaths in IT and programming increased by

46%

Office for National Statistics, 2012
Business Demography, UK: Bulletin

The Opportunity

As the economic impacts cause the pace of procurement to slow, an opportunity arises for your procurement and security teams to review their supplier assurance and due diligence processes.

Now is the time to make improvements by taking advantage of the reduced pressure to move suppliers through the onboarding process. An ineffective assurance process can add months of delay onto procurement cycles, but this can be dramatically reduced with an enhanced and streamlined operation using a tool such as the Risk Ledger platform (video).

Meanwhile, it gives your security team downtime to catch up on the backlog of suppliers whose security controls they have been unable to review in a meaningful way. Fewer than 50% of organisations have a comprehensive inventory of all their suppliers and only a minority proportion regularly review or monitor the security controls implemented by suppliers with whom they share confidential or sensitive information[1].

When an organisation does have a supply chain risk management programme in place, only 5% to 10% of their suppliers currently fall into scope, leaving unknown, unmanaged risks lurking in the vast majority of their supply chain.

During this period, there may also be the opportunity to renegotiate contacts with suppliers. This opportunity should be used to improve the contractual obligations on the supplier to have a good base level of security.

The next section sets out how any organisation can take action to capitalise on these opportunities and effectively manage the highlighted risks.

A good contract will oblige the supplier to engage with the risk assurance process, maintain the controls they attest to during the risk assurance programme and to run supply chain risk assurance themselves.

What do I need to do about these risks?

There are 4 key things your organisation's procurement and information security teams need to do to give you visibility of the risk, and to begin to mitigate it.

1. **Know who your suppliers are.**

   Your procurement team needs to ensure they have a database of all your contracted suppliers. If you do not have this database to hand, you can extract it from within your organisation's general ledger. This should hold a record of any suppliers that are currently being paid to provide services.

   Once you have this list, each supplier should be categorised by their criticality (how important they are to the functioning of your business) and the sensitivity of any data they may hold on your behalf. This information will allow you to build up an initial picture of your organisation's risk exposure.

2. **Run a risk assurance programme.**

   This is the only way to understand how the suppliers that hold data have mitigated the increased security risk and to assess the financial health of your critical suppliers.

   Once you know which suppliers have access to your data, your procurement and security teams need to understand whether they have implemented the correct controls to minimise the risk of a cyber-attack, and whether the critical suppliers are financially stable. This is done by running an assurance programme. During the COVID-19 crisis, particular focus should be placed on confirming your suppliers have enforced:

   - multi-factor authentication on public facing services;
   - the use of Virtual Private Networks (VPNs);
   - strong security awareness and training programmes for employees;
   - and effective patch management.

   Risk Ledger produces an open source framework to collect this data in a standardised way, covering all the controls that constitute a good base level of security and stability. It is important to review 90+% of your supply chain because less critical suppliers are more likely to be compromised and used as part of an attack vector to their clients.

   For example, a PR agency may not be considered a critical supplier but an email with an attachment from them will be trusted and opened by corporate clients without hesitation. If a supply chain is larger than 50 suppliers, it is advisable to use a tool to manage your assurance programme in an efficient way.

3. Brief the board.

Your board or senior management will be making strategic decisions to manoeuvre your organisation through the COVID-19 crisis. They need to be made aware that the crisis is causing an increase in supply chain risk, and they need to know the extent of the exposure and what steps are being taken to mitigate it.

It always helps to brief the board in financial terms. Describe the financial consequences of one of your critical suppliers suffering a data breach. Express the operational impact of one of your critical suppliers failing.

This provides a quantifiable understanding of an otherwise abstract risk and gives a baseline for prioritising it against other business risks.

4. Form a crisis team to effectively react to supply chain incidents and develop an incident response plan for critical suppliers.

A crisis team should be formed of both security and procurement professions that can assess the current visibility of supply chain risk and the mitigation processes that are in place.

They should then have the power to rapidly react to any incidents that do occur within the supply chain. The crisis team should update the board regularly on the risk to the business and the steps being taken to mitigate it.

The team should also create detailed continuity plans that outline alternative suppliers who can maintain critical services should any of your current suppliers fail.

Conclusion

Organisations need to have a good understanding of the security and financial posture of their supply chains, and this need is only amplified during the COVID-19 crisis and associated financial uncertainty.

To mitigate these risks, there are a number of key actions your procurement and security teams can take now: know who your suppliers are, run assurance over them, brief the board and form a crisis team empowered to manage issues. Those who don't are exposing themselves to serious and potentially existential risks such as considerable financial repercussions and long-term reputational damage.

This period of decreased procurement volume can be an opportunity to strengthen existing supply chain risk management processes, remove friction, maximise business value, and enhance supply chain resilience.

References

1. Ponemon Institute, 'Data Risk in the Third-Party Ecosystem', November 2018
2. Information Commissioner's Office, 'Penalties'
3. IBM, 2019 Cost of a Data Breach Report
4. Rob Lefferts for Microsoft, Microsoft shares new threat intelligence, security guidance during global crisis
5. ZDNet, VPN usage surges during COVID-19 crisis as millions work remotely
6. Gallagher, 'SMEs In An Age Of Crises: The need to bolster resilience to protect the UK's economic heartland', 2019
7. Risk Ledger Aggregated & Anonymised Supplier Assessment Data
8. Patricia Sabga for AlJazeera, 'Coronavirus economy: Recession or depression?' 2020
9. Office for National Statistics, 'Business Demography, UK: Bulletin', 2012

Risk Ledger Ltd,
7-10 Adam St,
London,
WC2N 6AA,
United Kingdom

Published May 2020

www.riskledger.com