Securing the Partner Ecosystem

Are Small Businesses the Largest Risk to Supply Chain Cybersecurity?

An (ISC)² Research Report

TABLE OF CONTENTS

INTRODUCTION

For many businesses, the supply chain represents one of the most vulnerable aspects of their entire operation, and giving up any measure of control over sensitive data is a necessary evil to be approached with caution. The 2018 "Data Risk in the Third-Party Ecosystem" study from the Ponemon Institute and Opus revealed that 59% of security and risk professionals across the U.S. and the U.K. said their companies had experienced a third-party data breach.[1] A separate study from Tenable, titled the Ponemon Institute Cyber Risk Report, found that misuse or unauthorized sharing of confidential data by third parties was the second biggest security worry for 2019 among IT professionals.[2]

Conventional wisdom has long held that small businesses have less sophisticated cybersecurity defenses, smaller budgets and fewer skilled resources, providing an easy entry point for hackers into large enterprises[3]. New research contradicts this belief. (ISC)^2, seeking to understand the level of threat posed to large enterprises by third-party partners, polled 709 respondents, half of whom were from small businesses with 250 or fewer employees, and half of which were from large enterprises with at least 1,000 employees.

The study found that large enterprises as a whole are conflicted about how much risk small businesses really pose. Only half of enterprises view their third-party partners as a cybersecurity risk, and even fewer (32%) say they have suffered a breach caused by a third party. When that has occurred, the breach is just as likely to have been caused by a large partner (54%) as by a small business (46%).

HANDING OVER DATA ACCESS

Almost two-thirds (64%) of large enterprises outsource at least 26% of their daily business tasks, which requires them to allow third-party access to their data. Outsourced functions vary widely and include research and development, accounting, IT services, accounts payable, customer services and advertising.

STATS ON SMBS

- According to the U.S. Small Business Administration, there are 28.8 million small- to medium-sized businesses (SMBs) in the United States, making up 99.7% of all U.S. companies[4]
- The 2018 Verizon Data Breach Investigation Report indicates that SMBs are the top target for cybercriminals[5]
- The Ponemon Institute's 2017 State of Cybersecurity in Small & Medium-Sized Businesses report found that the percentage of small businesses that experienced a cyber attack rose from 55% in 2016 to 61% in 2017.[6]

The overwhelming majority of enterprises (96%) has contract provisions specifying how third parties access, store and transmit their data. Additionally, 95% have a standard process for vetting small business suppliers' cybersecurity capabilities before providing them with access to their systems, which in some cases store and process sensitive data, such as personnel records and proprietary information.

Perhaps because of this vetting process, confidence runs high among enterprises regarding their small business partners' security practices, with 57% saying they are "confident" and 37% "very confident" in the cybersecurity measures their partners employ.

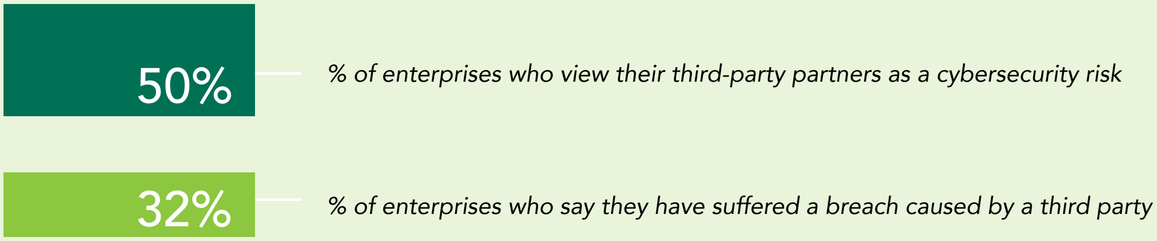
WHEN BREACHES HAPPEN

Not surprisingly, small businesses themselves do suffer security breaches. According to the study, 40% of them have experienced at least one. Additionally, one third (33%) of small business respondents admit that one of their employees has mishandled a client's credentials and 41% have had to notify a large enterprise client to reset a password as a precaution due to a security breach of the small business' systems.

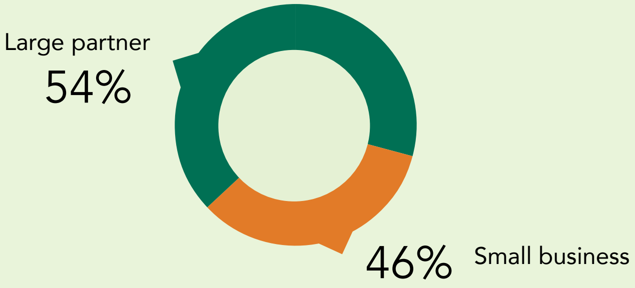
But while there are certainly instances when small businesses also cause breaches of large enterprise client data, the frequency of such events is fairly low. Only 19% of small business study participants say they have caused a data breach to a large partner. Moreover, an even smaller percentage (just 14%) of large enterprise respondents indicate that a small business partner has caused a breach , compared with 17% who say they were breached as a result of working with a larger partner.

> “Only 19% of small business study participants say they have caused a data breach to a large partner. Moreover, just 14% of large enterprise respondents indicate that a small business partner has caused a breach.”

RISK FROM THIRD PARTIES



Who was the third party breach caused by?



While one third of enterprises say they have suffered a breach due to a third party partner, still only half see these partners as a risk.

ASSIGNING BLAME

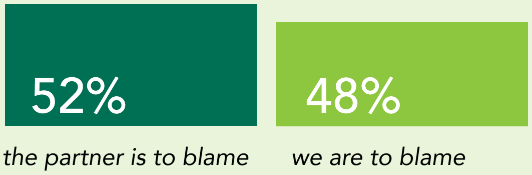
Despite high confidence in small partners to do the right thing, most enterprises aren't taking cybersecurity for granted. They will put partners on the spot if they have to, as evidenced by the finding that 60% of large enterprises have asked a partner why certain data was accessed. And when it comes right down to it, 69% of enterprises would hold a third party fully responsible for a data leak or breach caused by mishandling of their data.

Small businesses have no delusions about their position should a large client suffer a breach, and indicate that they have a high sense of accountability. 73% of them say they would feel liable if a client was breached, even if their actions only indirectly led to the security incident.

Still, there's no consensus on who is ultimately at fault for a breach caused by a third party. Even though enterprises are perfectly willing to hold third parties accountable for breaches caused by the latter, that doesn't mean enterprises will always assign blame to somebody else. In fact, nearly half of them (48%) would consider themselves "ultimately at fault" for a data breach caused by a third party, while the rest would blame the partner.

WHO IS ULTIMATELY AT FAULT FOR A DATA BREACH CAUSED BY A THIRD PARTY?

Enterprise respondents say:



LOOKING IN THE MIRROR

Nearly all enterprise respondents in the study seem confident in their own ability to fend off attacks. A full 98% are "confident" (54%) or "very confident" (44%) they can protect their data even if a third-party supplier is breached.

This may display overconfidence, however, considering 34% of large enterprise respondents say they have been surprised by the broad level of access a third-party provider had to their network and data. An even higher number of small businesses (39%) express the same surprise regarding access they have been granted to their large clients' data stores.

Yet, when alerted by a third party of insecure data access policies, 35% of enterprise respondents say nothing improves and 29% of small business respondents confirm this. Often, access remains unchanged even when the small business no longer needs to touch the data. More than half of small businesses (55%) have discovered they still had access to a client's network or data after completing a project or contract. This is a significant risk because orphan accounts – those no longer actively used – can lead to data breaches.[7] It's also an easy risk to address, since all it requires is the removal of the account.

The high level of confidence by large enterprises in their own security safeguards also seems misplaced as the study shows that more than half of small businesses (54%) have been surprised by some of their enterprise clients' inadequate security practices and 53% have notified large clients of security vulnerabilities they've discovered.

WHO WE TALKED TO

(ISC)^2 surveyed a total of 709 respondents from both small businesses with 250 or fewer employees (354 respondents) and large enterprises with at least 1,000 employees (355 respondents).

All respondents say they have visibility into how their organizations manage data, information, software and cybersecurity. They also all have influence or decision-making authority in selecting third-party vendors.

All of the enterprise companies grant access to parts of their network to third parties, and all of the small businesses provide services to large enterprises.

SIMILAR BEST PRACTICES

The tools and practices a company employs to protect its network and data significantly contribute to its level of confidence in preventing security breaches. The research shows that although they may have differing toolsets, large enterprises and small businesses tend to rely on similar best practices to protect their networks and data. Below are the top five security best practices employed by each group:

Enterprises:

1. Regular automatic scans with antivirus and anti-malware programs (68%)
2. Blocking access to known malicious IP addresses through firewall configuration (64%)
3. Strong email filters to prevent phishing (59%)
4. Evaluating and reporting on security incidents when they occur (59%)
5. Determining acceptable threat levels and employing encryption for sensitive data (57%)

Small Businesses:

1. Regular automatic scans with antivirus and anti-malware programs (71%)
2. Blocking access to known malicious IP addresses through firewall configuration (66%)
3. Strong email filters to prevent phishing (62%)
4. Scan all incoming and outgoing emails to detect threats and filter executable files (60%)
5. Evaluating and reporting on security incidents when they occur (48%)

Small businesses did confirm that they are limited by budget constraints. 72% indicated that there are other security tools they would invest in if they had additional budget resources.

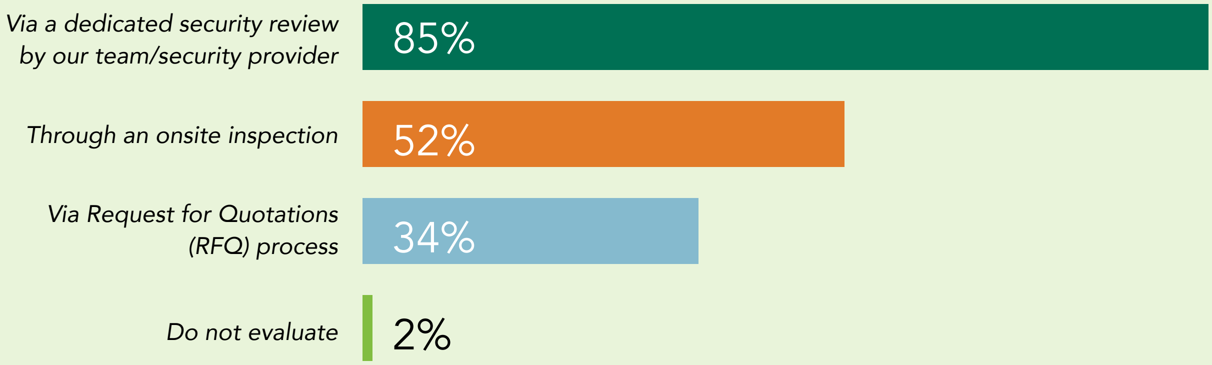
CYBERSECURITY TEAMS

The (ISC)² study also addresses another commonly held notion – that small businesses don't hire enough cybersecurity staff. In fact, the study shows that nearly half (42%) of small businesses employ at least five dedicated cybersecurity staff.

This compares with 75% of large enterprises that employ at least 10 staff members dedicated to cybersecurity.

Proportionally, many small businesses employ a higher percentage of cybersecurity professionals than their enterprise counterparts. For example, a 5-member cybersecurity team at a 250-employee company represents a greater percentage of specialists than a team of 10 at an enterprise with 1,000 employees or more. This data certainly calls into question any claim that small businesses, as a whole, do not take cybersecurity seriously enough.

HOW DO LARGE ENTERPRISES EVALUATE A VENDOR'S SECURITY CAPABILITIES?



CONCLUSION

The (ISC)^2 research shows that small businesses' reputation as the easiest conduit for bad actors to access the systems of large enterprises is most likely exaggerated, and that enterprises are just as likely to be breached through a relationship with a larger third-party supplier.

Especially telling is that enterprises themselves seem to recognize this, which is why there is no overall consensus among enterprises to be overly concerned about smaller partners than larger members of their supply chains - unless it can be proven they are at fault. It's also clear that enterprises need to improve their security practices in some critical areas, specifically in relation to addressing security issues discovered by partners and removing access to systems when partners no longer need it.

Breach prevention responsibility rests with all parties in a partnership, and enterprises should have the proper layered security controls in place to defend themselves from all angles of attack. Scapegoating small business partners may seem convenient, but enterprises need to be aware that in the eyes of their customers, it's their own reputations that are at risk and the buck stops with them.

How can these organizations improve their approach to shore up their defenses? A 2018 study by (ISC)^2 found that companies who successfully recruit and maintain strong cybersecurity teams – and are by extension more confident in being able to defend their information systems – do it by fostering a resilient culture of cybersecurity in which executives understand and reinforce the importance of security practices, hire certified security professionals, train and promote from within and draft clear job descriptions when hiring.[8] Creating a strong culture focused on cybersecurity is a core element in raising the bar of cyber competence and readiness, no matter the size of the organization.

In the end, size isn't the best indicator of a company's cybersecurity abilities or likelihood of being breached. It's everyone's joint responsibility to do their due diligence in working with partners when shared access to networks is concerned.

ENDNOTES

[1] Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks
https://www.apnews.com/556444d2cc114ea9a8ceda8f747b329c

[2] What is a supply chain attack? Why you should be wary of third-party providers
https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html

[3] Ponemon Cyber Risk Report
https://www.tenable.com/ponemon-report/cyber-risk

[4] U.S. Small Business Administration Small Business Profile report
https://www.sba.gov/sites/default/files/advocacy/United_States.pdf

[5] 2018 Verizon Data Breach Investigation Report
https://enterprise.verizon.com/resources/reports/dbir/

[6] 2017 State of Cybersecurity in Small & Medium-Sized Businesses report
https://csrps.com/Media/Default/2017 Reports/2017-Ponemon-State-of-Cybersecurity-in-Small-and-Medium-Sized-Businesses-SMB.pdf

[7] Want Better Identity Management? Remove your Orphaned Accounts
https://solutionsreview.com/identity-management/want-better-identity-management-remove-your-orphaned-accounts/

[8] Building a Resilient Cybersecurity Culture
https://www.isc2.org/Research/Cybersecurity-Culture

METHODOLOGY

Results presented in this report are from an online survey conducted by (ISC)[2] and Market Cube in November 2018. The total respondent base of 709 IT/ICT/cybersecurity decision makers included 354 from small businesses with 250 or fewer employees and 355 from large enterprises with at least 1000 employees, all based in North America.

ABOUT (ISC)[2]

Celebrating its 30th anniversary this year, (ISC)[2] is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)[2] offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, more than 140,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

For more information on (ISC)[2], visit www.isc2.org.

(ISC)^2®