

Cyber risk and moving beyond "the cost of doing business"

Derek Johnson
Reporter/Editor, SC Media

The biggest attacks target software supply chain and high-level access

SC MEDIA TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Uber confirms hack in the latest access and identity nightmare for corporate America

[Derek B. Johnson](#) September 16, 2022



SC MEDIA TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Feds arrest teen Twitter hack leader, accomplices


[Teri Robinson](#) July 31, 2020

The ringleader of the Twitter breach that used prominent accounts to run a cryptocurrency scam turns out to be a 17-year-old in Tampa arrested earlier today.

SC MEDIA TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

The lesson from Kaseya: so-called 'solutions' can become big problems

July 16, 2021



SC MEDIA TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Government briefed on breach of at least 30,000 Microsoft Exchange Servers

[Joe Uchill](#) March 6, 2021

Government officials have been briefed on a major investigation that has led to the discovery of a breach of at least 30,000 Microsoft Exchange Servers.

Business is getting more (not less) complex

- IT modernization has helped businesses compete in a modern, fast-paced environment, but it also dramatically increases an organization's attack surface
- COVID-19 supercharged this trend and put a lot of businesses with immature security online
- "There's actually new risk drivers beyond the typical Verizon data breach report, and those new risk drivers are really all around digitization and the desire by boards to essentially increase their risk appetites. They literally want to take on more risk in pursuit of mostly digital initiatives." - John Button, Gartner

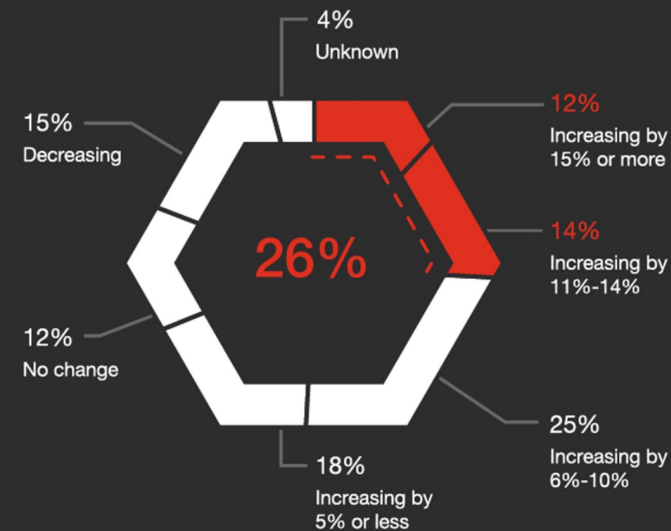
Business is getting more (not less) complex

private networks and sensitive databases, and they rely on them for everything from expense reporting and email services to managing industrial control systems. More than one-third of participants in this study had at least 100 third-party relationships, with some sectors, such as healthcare and government, working with 500 or more vendors at any given time.

Each vendor has the potential to create additional vulnerabilities by expanding the number of entry points into an organization's digital footprint. Yet most organizations lack the continuous visibility and knowledge of the security risks these third-party networks present. As a result, 91% of respondents had experienced a security incident related to a third-party and expressed some level of concern with experiencing another breach or falling out of compliance due to a partner vulnerability during the past 12 months.

Source: Cyber Risk Alliance & Security Scorecard

More than 25% expect double-digit growth in cyber budgets in 2022

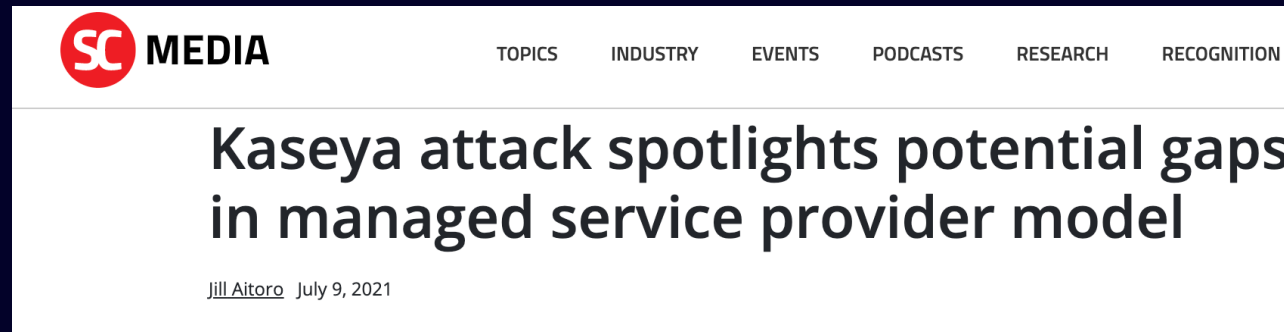


Source: PwC 2022 Global Digital Trust Insights Survey

If your security program can be beat by a motivated teen, it's not "advanced"



1000 compromises, one “weakness”



“They have an issue here, because MSPs are responsible for their customers. And Kaseya provides this service that the MSPs pay for,” said Dede Haas, channel strategist at DHL Services and an expert in MSP models. “There’s a chain of trust that has now been broken.”

“What should be happening now, is for every customer to assume that all their MSPs have been compromised, and to implement compensating controls within their own enterprises to properly segment the data exchange,” she continued.

Beyond the breach

- These hacks don't just impact systems and data, they undermine the legitimacy of entire security programs
- They open companies up to greater scrutiny by insurance companies
- They underpin lawsuits that question the company's very commitment to security and honesty with shareholders + government

Courts are open to the argument



breach was not the same server that was compromised in the breach at issue here. Plaintiffs need not plead that the password incident directly caused the later breach—instead, they need merely demonstrate that Defendants were knowledgeable or at least reckless with their statements regarding SolarWinds’ security, that Plaintiffs relied on Defendants’ commendations of SolarWinds’ security,

among other things. (*Id.* at 5). A photo and video of Brown was featured prominently near the Security Statement, and Brown likewise regularly wrote articles and appeared in interviews and on podcasts touting SolarWinds’ focus on “heavy-duty hygiene” and directing customers and investors to the Security Statement. (*Id.* at 5, 18–19). SolarWinds’ commendations of its cybersecurity measures “helped the Company build up its customer base,” “as it gained 300,000 customers worldwide and more than \$230 million in federal government contracts” during the class period. (*Id.* at 5).

Three possible explanations

- 1.) This is just the cost of doing modern business, so make peace with it
- 2.) Organizations are just being lazy and don't prioritize security, so do that
- 3.) Our current model of incremental improvement and additional complexity is the best way to manage

Will it get better?

Pessimistic:

- “We’re chasing a little bit after the last thing and not taking a longer view. Now there are 20 things you need to do instead of 15 and we’re still allowing for some fundamental level of insecurity. I just don’t know that I’m optimistic that that paradigm shift is occurring yet.” – Bob Kolasky, former NRMCM director at CISA
- “I think it’ll get worse before it gets better. Largely because there may not be the incentives yet to really give it a college try to fix this stuff.” John Button, Gartner

Optimistic:

“Good risk analysis is not perfect, it’s not a perfect science, no one is saying it is, but it’s better than what we were doing yesterday, it’s better than what we’ve been doing for the last 10 years.” - Zach Cossairt, Equinix

Thanks for listening!

Derek B. Johnson

SC Media

Derek.johnson@cyberriskalliance.com

www.scmagazine.com