nccgroup

Shutterstock: royalty-free stock vector ID: 246371155

Dec 11, 2019 16:48 GMT

Trust, but verify (your third-party vendors)

By Sourya Biswas, Technical Director, NCC Group

As far back as 2010, Google estimated that more information was being created every two days than had existed in the entire world from the dawn of time to 2003. Granted, a lot of this information included cat videos and the like, but there's no denying that this proliferation of information has led to specialization of knowledge because the human mind can only know so much.

Benjamin Jones, an economist at the Kellogg School of Management at Northwestern University, explains it well: "Once upon a time you could be a biologist. Now the accumulation of knowledge is such that biologists, for example, must specialize in an array of micro-disciplines like evolutionary biology, genetics and cell functions. At the turn of the 20th century, the Wright brothers invented the airplane; today the design of the jet engine calls upon 30 different disciplines requiring a vast array of specialized team."

Similar to what Benjamin Jones was saying, this phenomenon of specialization is all too evident in the corporate world. This, in turn, has led to an explosion of third-party suppliers and vendors to meet business needs. For a company focused on core operations and meeting the needs of its stakeholders, it makes financial sense to handover non-core functions to third-party vendors. Unfortunately, this introduces a whole new element of risk in the company's ecosystem – third party risk, of which cybersecurity is a critical component.

Even as companies recognize the ever-evolving threats to their immediate operating environment, they often ignore the protection of data or access to internal systems provided to vendors. While some organizations do specify cybersecurity requirements as part of their vendor evaluation process, there's often pushback, both from within and outside, on what can or cannot be imposed on vendors.

Breaches through third parties are among the most highly publicized.

Even for those that have documented third-party security requirements, enforcement is often lax. The result? Some of the most notorious data breaches of recent times have occurred as a result of the organizations' vendors.

Target: Over the last two months of 2013, hackers stole data including 40 million customer debit and credit cards. The breach, noticed in Feb 2014, was traced back to network credentials stolen from HVAC provider Fazio Mechanical Services that were used to implant the malware "BlackPOS" (a.k.a. "Kaptoxa") across Target's Point of Sale (POS) terminals. Target reported that the total cost for this compromise was $291 million before insurance adjustments.

Home Depot: In Sept 2014, the DIY retailer was hit by a variant of the

malware used to attack Target, with the infiltration again being traced back to compromised third party credentials. In addition to 56 million credit and debit card details, 53 email addresses were also leaked. Total cost of the breach before insurance pay-outs was $263 million.

DoorDash: In Sept 2019, the food delivery company disclosed a breach that occurred in May and compromised 4.9 million records; information leaked included email addresses, delivery addresses, order history, last 4 digits of payment cards and drivers' license numbers. An "unauthorized third party" has been blamed, but details are lacking.

While not technically a data breach, the Verizon incident of Jun 2017 saw six million customer records exposed by a third party on a misconfigured AWS S3 bucket. This is interesting because the company also publishes the authoritative Data Breach Investigations Report (DBIR), proving that even mature organizations are not immune to third-party cyber security risks. This is not unexpected since an attacker only needs to be right once, while the defender has to be right all the time.

There is heightened awareness around third-party risk.

Based on our Threat Modeling exercises, one in three companies have confirmed a third-party attack vendor as the source of an issue they have encountered. The 2018 "Data Risk in the Third-Party Ecosystem" study by the Ponemon Institute that surveilled more than 1000 CISOs revealed that on average, companies share confidential and sensitive information with approximately 583 third parties; however, only 34 per cent maintain comprehensive inventories. As many as 63 per cent of the respondents believe they lack resources to manage third party relationships; only 35 per cent rated their third party risk management programs as highly effective

While these statistics are alarming, it's a positive that most security stakeholders are aware of their shortcomings in managing third-party risks. As we have all heard, "The first step in solving a problem is recognizing there is one." Once the ball is set rolling, there's a need for establishing clear metrics ("you cannot manage what you cannot measure") and continuing to improve ("continuous improvement is better than delayed perfection") the process in a circular feedback loop.

As far as management of third-party risk is concerned, not all companies are

the same—they have different sizes, different vendors handing different products and services, different resources and budgets to manage risks, and different timelines to meet. In other words, flexibility is key to success.

In addition, leveraging a modular approach is key, with specific actions around development, implementation, assessment, management, and improvement. As far as vendor risk is concerned, our mantra is, to quote Ronald Reagan, *"Trust, but verify."*

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750

Regional Press Office - Europe
Press Contact
foxit@mcspr.nl
+31 (0)23 562 8208