Tackling Cyber Security in a World of Digital Ecosystems

Author

Sundeep Oberoi

Global Head, Information Risk Management, Tata Consultancy Services

Companies across the world realize they are operating in digital ecosystems, constellations of players that are erasing once-sacrosanct boundaries of age-old industries. They are relying on these ecosystems to both sell products and services and to buy them—and the transactions are with not only traditional allies but also potential competitors.

But, what too firms many aren't aware of is the rising risk of cyber attacks when they digitally connect their systems and data to those of other companies. While the answer is not to disconnect from these ecosystems, the risks of playing need to be understood and lowered considerably.

In the old 'physical' world in which companies interacted by making phone calls, sending invoices and payments through the mail, and conducting meetings in rooms, the risks of such collaboration were much smaller. There are limits to the number of customers you can reach, the number of people you can employ, the number of businesses you can partner with, the amount of information you can store, and the number of products and services that you can offer.

By contrast, in the digital world, there are no such limitations. In fact, it is a world of infinite possibility, with an abundance of capital, talent, capabilities, and businesses with which to partner.

To prosper in a world of digital ecosystems, companies will need to change not only the ways they interact, but they also must alter the security procedures they put in place to guard their systems, data (especially customer data), and digital infrastructure they hand over to the companies that manage public clouds.

Moving Into Ecosystems: There's No Stepping Back

If you think the way to manage this risk is to stay out of the digital ecosystems that have formed in your sector, think again. Already, many leading companies are embracing ecosystems. Take Ping An. The world's largest insurer, this Chinese company, founded 31 years ago from state institutions, is morphing into something quite different by creating technology-driven businesses alongside its traditional financial services. It has become what we call 'an ecosystem orchestrator,' investing 1% of annual revenue—about $1.5 billion—in building a technology platform. Using artificial intelligence, big data and analytics, and automated services, Ping An has used the platform to launch: financial services, an online car marketplace, and an online medical consultation service for Chinese patients. Who would have thought that a once-staid insurer, whose name translates as 'safety,' would be in the health clinic business?[36]

That kind of cross-over business is becoming the norm in the world of digital ecosystems. It is already starting to pay off. Ping An has created new sources of revenue and new sources of customers for its core insurance and banking

[36] Financial Times, "Ping An's hedge against future risks," November 10, 2018, accessed August 9, 2019: https://www.ft.com/content/6db6ed90-d6b5-11e8-a854-33d6f82e62f8.

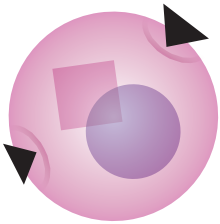
Companies that put their digital capability at the heart of their enterprise are beginning to pull ahead of their traditional rivals.

businesses. In 2017, 40% of new financial services customers came from its ecosystem businesses.[37]

Other companies that put their digital capability at the heart of their enterprise are beginning to pull ahead of their traditional rivals. Our research on more than 1,000 North American and European companies shows that in 2018, the digital leaders attributed 63% of their revenue to their digital businesses or digital products and services—far higher than 'follower' companies, which only attributed 38% of their revenue to digital businesses or digital offerings.[38]

But there is a catch, and that catch is new cyber risks.

Friend or Foe? The Risks of Joining a Digital Ecosystem



Ecosystems are not just networks of friends. They are networks that can include rivals, too. Although companies have long had to collaborate with their competitors—the language of 'frenemy' is nothing new—the way they now have to collaborate is altogether different to the way they once had to in the pre-digital past.

These days, when two companies interact within an ecosystem—where several different organizations own and manage different parts of what is, by definition, an interoperable system—they are necessarily required to

[37] Ibid.

[38] Tata Consultancy Services, "TCS 2020 CIO Study: Digital Leadership for Business Transformation". https://sites.tcs.com/bts/wp-content/uploads/TCS_2020_CIO_Study_Preview_v5.pdf. Accessed August 9, 2019.

share some of their most important data. That's just a cold fact of collaborating in the digital sphere. But, as a result, they increase the likelihood that they could become the victim of cyber security attacks.

All companies collect data about their customers, and so long as they have an appropriate cyber security defense, they can meet their regulatory obligations and ensure the security of this data. But the challenge of doing this rises significantly when they participate in an ecosystem. In this digital environment, they are no longer fully in control.

They have to rely on the security guarantees of their partners—which might be suppliers of components, cloud services, customers, marketing, and many other goods and services—and, of course, they cannot independently ensure that.

There is evidence that companies are struggling to contain the emerging cyber security problem. In 2018, according to the Identity Theft Resource Center, which tracks the incidence of scams, fraudulent activity and cyber theft, there were 1,244 breaches of data. The reported number of exposed consumer records containing sensitive, personally identifiable information jumped 126% to 446 million from 197 million in 2017.[39]

Such security breaches are likely to increase over the coming years, for two reasons. First, companies face a relentlessly moving target because the speed with which malware and other computer hacking technology is being developed is simply outpacing the speed with which they can develop adequate responses. Some 350,000 new malicious programs and potentially unwanted applications are registered by cyber security firms every day.[40] By the time companies have found a way to close a hole in their security wall, another hole opens up.

Second, different countries have different ways of responding to, investigating, and prosecuting cyber security incidents. In October 2015, for example, the European Court of

[39] CyberScout, "Consumers at Risk: 126% Increase in Exposed Consumer Data, 1.68 Billion Email Related." January 28, 2019. Accessed August 9, 2019. https://www.idtheftcenter.org/consumers-at-risk-126-increase-in-exposed-consumer-data-1-68-billion-email-related-credentials/.

[40] AVTest, "Malware". Accessed August 9, 2019. https://www.av-test.org/en/statistics/malware/

Justice struck down the 'Safe Harbor' data-transfer provision of the 1995 Data Protection Directive amid fears over U.S. surveillance. (The Safe Harbor rule had permitted companies outside the EU to store and process the data of Europeans.)

Realizing they were moving on divergent paths, the EU and U.S. worked furiously to strike a compromise that would restart the vital flow of data across the Atlantic. The new deal—the EU-U.S. Privacy Shield—requires American companies wishing to import data from Europe to meet new obligations on processing personal data and guaranteeing individual rights. But the episode serves to illustrate that regulatory disunity further complicates risk management for corporate leaders.[41]

How to Reduce Ecosystem-Related Cyber Security Risks

The risks of participating in digital ecosystems are very real. But they should not be feared. Indeed, we think the risks of not participating in an ecosystem are arguably greater. Companies that continue to view their customers, competitors, and business partners through the lens of a single industry will be far less able to recognize the new types of customers, competitors and business partners with which they will need to interact as businesses increasingly go digital.

Given this, it is incumbent upon senior executives to address the cyber security risks head on. How can they do this?

From our experience, companies should consider taking several measures to strengthen their cyber security capabilities.

[41] World Economic Forum, "Global Agenda Council on Cyber Security," April 2016. Accessed August 9, 2019. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf.

Before joining a digital ecosystem, they should carry out the same kind of due diligence review of potential partners—especially those considered competitors—that they conduct when making an M&A transaction. Since large companies began years ago allowing vendors to access their IT systems, they have performed vendor risk assessments. These assessments examine the vendor's business practices and evaluate them for the risk they present to the company. Companies can extend that same principal to their ecosystem interactions: assess the risks associated with any ecosystem entity that is technically connected to a company, or shares data with it.

While they are reviewing their partners, companies should introduce a series of safeguards to facilitate the secure automated exchange of data with prospective partners. At the heart of any digital ecosystem is machine-to-machine communication—computers and digital sensors communicating with one another. This raises the bar for cyber security: Conventional passwords and two-factor authentication offer scant defense in a hyperconnected environment where artificial intelligence and machine learning allow commercial rivals with malevolent intentions to stay one step ahead.

Here are some protective steps that companies should take:[42]

- Build new gates that require the machines to present the right credentials—some form of a digital identifier—so that a machine can verify that another machine has access rights. Cryptography, in which automated parties exchange digital signatures to authenticate their interactions, is one way to do this.

- Ensure that every company asset—even the humble office printer—has its own authentication process. In other words, the traditional system, where a single administrator can access multiple devices on a corporate network, needs to be scrapped. This might sound like an extreme reaction, but the fact is that hackers make it their business to seek overlooked assets that provide a backdoor entrance to a company's entire network.

[42] Thiagarajan, Satish, "Three Ways to Secure Your Automated Machines," https://sites.tcs.com/bts/three-ways-to-secure-your-automated-machines-blog/. Accessed August 9, 2019.

- Turn the digital hackers' weapons on them by using artificial intelligence and machine learning to develop systems that analyze various threats—network intrusions, distributed denial-of-service attacks, viruses in emails, phishing scams—and identify patterns of behavior.

These measures will go a long way toward protecting a company. But business partners, clients, and customers will want to be reassured that the company has put in place well-designed controls that protect sensitive personal and commercial data.

As such, senior executives should commission an external review of their company's non-financial reporting controls—the security, availability, processing integrity, confidentiality, and privacy of a system. Such a review—known as a Service Organization Control 2, or SOC 2, audit—provides a report on the description of the controls, attests that they are well designed and implemented at a specific point in time, and further attests that they are operationally effective over a minimum six-month period.[43]

With careful due diligence, appropriate protection, and an external audit that provides peace of mind, a company can go a long way to addressing the cyber challenges they face in digital ecosystems. But it remains a fact that, however high a company builds its security walls, it will almost certainly suffer some loss of sensitive data.

Digital ecosystems are here to stay, so it is imperative for companies to actively engage in them to create value for stakeholders.

[43] AICPA, n.d., https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html. Accessed August 9, 2019.

For this reason, companies must develop a sophisticated post-attack response. There are three key elements to this:

1. An enhanced cyber forensics capability that can gather, preserve, and analyze digital assets in a way that is useful for any future legal proceedings
2. Well-developed business continuity plans
3. Pre-prepared plans for regaining user trust

All Ecosystems Go: Tackle Cyber Security and Turbo-Charge Your Company

Digital ecosystems are here to stay, so it is imperative for companies to actively engage in them to create value for stakeholders.

But, of course, there are risks. An ecosystem is an interoperable system. Participation necessarily means giving up some control and relying on commercial partners to follow through on their commitments to be responsible in using data, systems, and other assets.

Fortunately, there are steps that companies can take to mitigate the risks. With constant vigilance, they can make it much more difficult for malevolent hackers to break through their security walls. Yes, they will need to make a significant investment of time and resources. But we are convinced that this investment will be more than repaid by the prize of participating in the ecosystem economy.