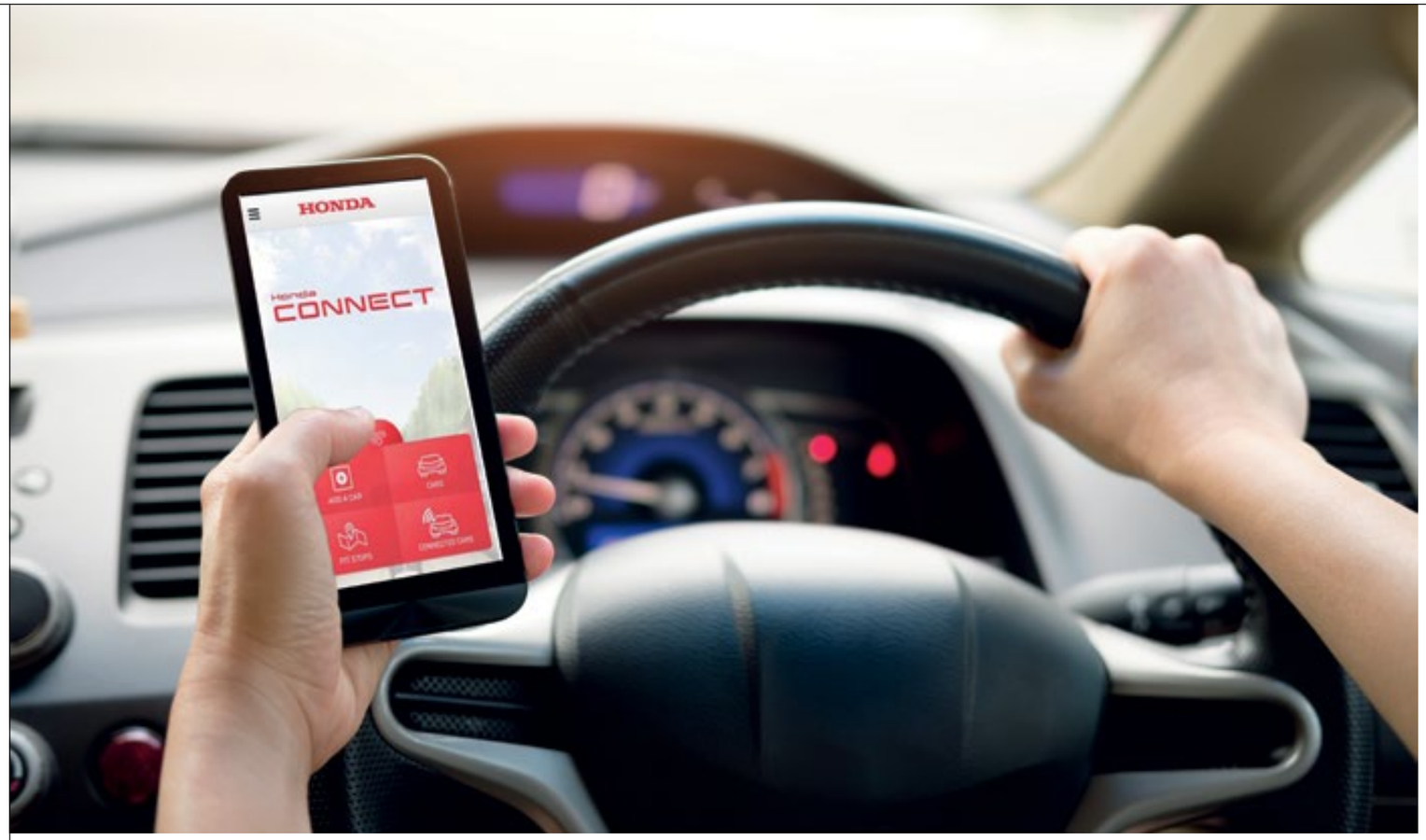


STOPPING THE RIPPLE EFFECT

Matthew McKenna *on the importance of setting the score with vendor risk management*

The modern business world is built on interconnectivity, with each organisation sitting within a complex web of customers, suppliers and partners. As companies continue to incorporate more digital services, such as cloud-based solutions, these connections have become ever deeper. This means that organisations must increasingly not only be mindful of their own security, but also the capabilities of almost every company in their web of connections. A security incident affecting one company will ripple outwards to potentially endanger every organisation that they are associated with.

Cyber criminals will frequently exploit these connections by seeking out vulnerable third parties with weaker security to bypass the defences of their real target. Some of the most significant breaches of recent years were the result of attackers purposefully going through a third party, and there have been numerous examples in 2018 alone. For example, in June, Ticketmaster detected malware in an online chatbot support service offered by a third party. The company was quick to disable the compromised chatbot, but tens of thousands of customers are still believed to have been at risk.

Server and cloud misconfigurations by third parties continue to be some of the most common causes of breaches. In one recent case, Universal Music Group had key data including AWS secret access keys, internal FTP credentials and SQL passwords exposed due to a contractor failing to secure an Apache Airflow server. In another incident, more than 50,000 users of the Honda Connect App had their data left at risk for over a year after a Honda affiliate misconfigured two Amazon S3 buckets.

50,000 Honda customers had their data put at risk thanks to a third-party affiliate

DUE DILIGENCE

The potential for a cyber attack through a third party means that having a Vendor Risk Management Programme in place for all suppliers should be a matter of course for any organisation. An effective programme not only needs to assess new vendors before contracts are awarded, but should also carry out due diligence and on-going monitoring for all existing vendors. But the depth and breadth of even an average-sized company's supply network makes this a difficult task.

Tackling this challenge requires an operationalised approach, with strict and consistent standard operating procedures (SOPs) to ensure that all assessments are thorough without making the process too resource heavy. Operationalising a Vendor Risk Management Programme begins with understanding the key elements and steps to take to translate processes into SOPs as well as how to identify and tier vendors.

Gaining a comprehensive understanding of the vendor landscape is an important first step to better risk management. This initially means mapping out the complete vendor selection and management process, including being aware of all of the stakeholders in each vendor relationship, inclusive of both individuals and business units within the organisation.

A Vendor Risk Management Programme can only work with regular involvement from vendor stakeholders, and it is important they understand the processes at work and what the potential risks of new vendors are. Outside those dealing directly with vendors, other critical stakeholders in the organisation include legal, procurement and information security.

There can be a big disparity between different vendors in terms of size, structure – and potential risk. To deal with this, businesses should establish a set of baseline intake questions for stakeholders to apply to each vendor. At a basic level this can include the vendor's name, products and services, whether it is on or off-premises and what kind of data it can access. Each vendor should also be categorised into a type, such as cloud, software, hardware or mobile, and its overall level of criticality to the business should be considered. Vendor stakeholders will play a key role in categorising vendors and gathering this data.

The next step is to map them to a tier of risk, generally running from one to five, with five being the highest level of risk. A tier one vendor would have no access to systems and data, and therefore pose little risk, while a tier five would be a critical vendor with access to essential systems, and capable of causing major disruption in the event of a security incident. It can also be beneficial to align these tiers with those of an existing enterprise risk management tier system. Following this, SOPs can be developed to apply to each level of risk, with more measures in place for those vendors deemed riskier. For example, vendors that are SaaS-based or offsite with access to sensitive data should be scored higher than on-premises solutions and appropriate SOPs should be in place to account for this.

Vendor Risk Management is sometimes conflated with a more general risk assessment of a vendor's implementation within the corporate environment. While there is some crossover and findings should be shared between the two programmes, it should be noted that the former focuses on a vendor's own security hygiene and capabilities rather than the impact of its operations.

It's important that the risk assessment is tailored to the risk tiers and vendor types established by the organisation, as using a generic approach will cause unnecessary friction for vendors and stakeholders alike. Attempting to use a one-size-fits-all format will mean that time is wasted on less relevant fields for some vendors, while critical risk areas are overlooked for others. For example, vendors that have no access to data and have a tier one or two designation could be given a self-attestation with a few questions to confirm basic assumptions such as no access to systems or data.

While it is important for the risk assessment to be a very open process that is carried out in cooperation with the vendors, a thorough evaluation should combine the vendor's self-assessment with external investigation. Non-intrusive research into sources including the public and dark web can yield essential indicators of risk that the vendor themselves may not be aware of. As a starting point, armed with a vendor's name and URL, it is possible to perform an initial review and compare its security hygiene to that of its industry peers. This information can provide a quick snapshot of the vendor, and a quick review can reveal some immediate red flags and provides a foundation for more thorough assessment.

IDENTIFYING VULNERABILITY

Scanning the open web can indicate a company's potential vulnerability to dangerous social engineering attacks by detecting factors such as employees using corporate account information for social networks, service accounts, personal finance accounts and marketing lists. Open web sources can also be used to determine the suppliers that any vendor is connected to. While the vendor itself may be secure, having ties with an insecure vendor could still heighten the risk to an organisation.

Even more information can be revealed by delving into the dark web. Tracking private hacker forums can reveal chatter relating to the vendor, indicating if it is being considered as a target. Continuous monitoring can also uncover any breaches and leaks that contain sensitive information concerning a vendor or its users accounts.

A vendor's potential risk level can also be assessed through its IP reputation. By monitoring malware signals from commandeered Command and Control (C2) infrastructure around the world, it is possible to determine the quantity and duration of malware infections at a particular company's IP address.

Organisations need to ensure that the results of their Vendor Risk Management Programmes are properly incorporated into their process if the scheme is to have any meaningful impact on security.

One of the most effective approaches is to include data security as a contract clause within a vendor's Master Service Agreement (MSA). Any vendor that stores or processes data on behalf of the organisation should have a clause on security risk as part of its service contract. In particular, vendors that are known to subcontract to other vendors need careful management to ensure they don't expose the company to undue risk through their own suppliers.

A thorough security assessment should be carried out before the contract is negotiated so that findings for the vendor's security posture can be included in its contractual obligations around the management and care of the organisation's data. Contractual language around security risks also needs to be very carefully worded, both aligning with the company's procurement and legal teams and incorporating input from the vendor's stakeholders.

OPEN WEB SOURCES CAN BE USED TO DETERMINE THE SUPPLIERS THAT ANY VENDOR IS CONNECTED TO

An organisation can link security risk management to the vendor's Service Level Agreement (SLA), with a vendor, therefore breaching its contract in the same manner as missed targets and timelines. Vendors can be given a specific strategy and timeline to address risk factors uncovered in the assessment.

A useful strategy is to develop a comprehensive general data security contract for use with all vendors, and then customise it based on an individual vendor's type and risk tier. Vendors in higher risk tiers will dictate more data security clauses to be included within the contract.

Finally, a 'right to audit' clause should be included in every data security agreement. This will go a long way towards ensuring a vendor is fully compliant with the assessment process and any later inquiries. Likewise, an annual vendor review can be included in the contract, and specific factors such as keeping systems patched can be included as criteria.

Continuous monitoring is recommended for the highest risk vendors and potentially even daily monitoring checks for tier-five vendors who are closely connected to the organisation's most critical systems and data. A review process should be in place to discuss issues and suggest mitigation steps if a vendor falls below the agreed security level.

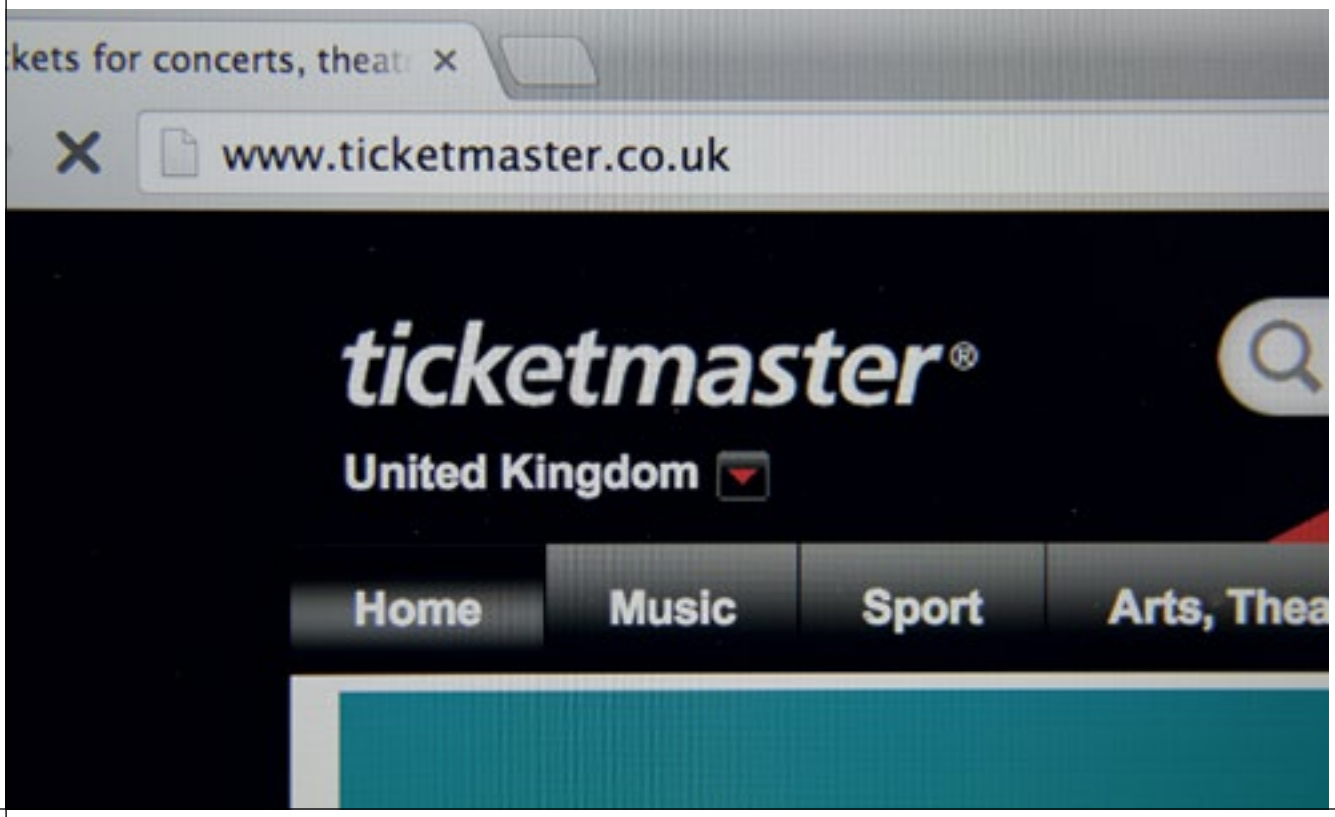
RECIPE FOR SUCCESS

A successful Vendor Risk Management Programme will play an essential role in reducing the risk to an organisation from its third and fourth party connections. While the business world is continuing to grow in complexity, establishing a programme based around a risk score for each vendor that reflects its type, security stance and access to key systems and data will make it much easier for a company to manage and assess its vendors.

By incorporating an in-depth analysis of internal and external factors to assess each vendor's risk level, businesses will be able to identify and mitigate potential threats before they can threaten the business. Continuous monitoring of high-risk vendors which includes both open and closed sources will also enable a company to spot new risks, potentially even before the vendors themselves.

Combining these abilities with a well-structured and consistent set of SOPs will ensure that a company can not only maintain a high standard of security through its connections, but is able to do so without damaging business relationships with a clear and open approach to vendor risk ●

Matthew McKenna – Vice President EMEA at SecurityScorecard – has extensive experience in the technology and security industry. Matthew is a high-energy strategy and operations executive with a track record of commercialising emerging technologies across sectors in global markets.



Ticketmaster's security was thrown into chaos by an online chatbot support service offered by a third party

Picture credit: Getty