Don't be your own worst enemy: protecting your organisation from inside threats


Jamie Tyler

Jamie Tyler, CenturyLink

Cyber-security spending is at an all-time high and shows no signs of letting up – the global market hit $75bn in 2015 and is set to increase to $170bn by 2020.[1] And this shouldn't come as a surprise. Cybercrime is on the rise, with theft of 'hard' intellectual property alone increasing by 56% just last year.[2] With each data breach costing a victimised organisation an average of $4m – not to mention the jarring impact on reputation and customer trust – it is no wonder that organisations are throwing so much money at the problem.[3]

While several recent high-profile hacks may lead you to believe otherwise, most data breaches are not the result of a mastermind outsider attack. In fact, only a quarter of data breaches are attributed to external hacks.[4] The vast majority are enabled by insider leaks, whether intentional or the result of seemingly innocent events, such as the loss of a corporate phone, or clicking on phishing or malware.

Globally, these types of incidents account for more than half of all data breaches.[5] Furthermore, inside jobs can be just as devastating as external ones – the infamous Panama Papers leak of over 11.5 million files is strongly believed to be the work of someone who at one point had legitimate access to the data.

Nevertheless, organisations are still more preoccupied with preventing external threats than internal ones. More than seven out of 10 organisations (71%) admitted that they were 'very concerned' with the possibility of an external attack, but less so (46%) regarding internal vulnerabilities.[6]

Mitigating insider threats is a different beast altogether. While all outside attacks can be labelled as malicious, premeditated events, insider breaches often result from human error or device loss. As such, organisations must protect their data using a two-pronged approach that addresses security through rigorous, ongoing employee training and implementing the right technology safeguards.

Greater employee access to sensitive information (such as customer data and financial figures) and increasingly connected organisations have resulted in more opportunities for employees to do their jobs more efficiently. But it's also paved the way for causing damage to their organisations.

Your organisation is only as secure as its weakest link. And if your weakest link is an employee, contractor or partner accessing sensitive company data via their personal device that is connected to other services for personal use or shared with non-employees, you could be in dire straits.

Today's digital culture doesn't make it any easier. Blocking all access to sensitive data or banning modern ways of working such as BYOD isn't the answer; by doing this, you may very well hinder the efficiency of your employees. HR and IT staff must collaborate to raise awareness of potential security threats and how to respond when confronted with suspicious events – for example, how to safeguard company data on personal devices or who to contact when they suspect they have been hacked. This may come in the form of required training or part of the induction programme to the company. Equally, new processes and internal governance must be put in place and followed through to ensure that safer habits are spread culturally throughout the organisation.

In preventing malicious or pre-meditated leaks, HR and IT must collaborate on how to vet employees for access to which

Continued on page 20...

...Continued from page 19

types of company assets. Cyber-security verifications can be embedded within typical background checks for prospective hires or an ethics test before handing over new responsibilities. This will help you identify the right candidates who can be trusted with sensitive data.

In protecting your organisation from insider threats, technology acts as the insurance. The first thing you should do is limit the potential damage caused by insider leaks. This translates to managing the individual privileges your employees have to specific data or services on the company network. This may include separate access tokens or having access policies that limit who, when, where and how specific company information is accessed.

Admin privileges should be examined more closely. For example, specific company data related to financial figures can only be accessed by pre-approved accounting staff during working hours, on approved company devices and within a certain mile-radius of company property.

Furthermore, regular audits with trusted external partners will help you cater the various access privileges appropriately for your organisation. This should be monitored alongside regular reporting on the status of company assets, identity of employees and logs of how long employees spent with these assets. Understanding these activities will enable your staff to identify anomalies in activity or weaknesses in security processes.

While technological and cultural shifts within organisations such as cloud computing, big data and BYOD have increased staff agility and efficiencies, they have also opened them up to a new world of vulnerabilities. Protecting sensitive data – customer information, financial figures and your company's reputation – is a critical part of any successful IT strategy. The risks of not implementing the right safeguards are enormous, ranging from potential lawsuits and significant fines to damaged reputation and, perhaps most importantly, the loss of customers.

By proactively educating staff and closely monitoring their permissions and activity on the company network, you can help prevent your organisation from becoming its own worst enemy while ensuring that employees still enjoy all the benefits of working for an innovative, forward-thinking organisation.

About the author

Jamie Tyler is director, digital transformation & innovation, at CenturyLink. With 24 years of experience in information technology, he has a thorough knowledge of cloud, visualisation, networking, compute and storage platforms.

References

1. Morgan, Steve. 'Worldwide Cybersecurity Spending Increasing To $170 Billion By 2020'. Forbes, 9 Mar 2016. Accessed Jul 2016. www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cyber-security-spending-increasing-to-170-billion-by-2020/#25728b1676f8.
2. 'The Global State of Information Security Survey 2016'. PwC. Accessed Jul 2016. www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html.
3. '2016 Ponemon Cost of Data Breach Study'. Ponemon Institute/IBM. Accessed Jul 2016. http://www-03.ibm.com/security/data-breach/.
4. Budd, Christopher. 'Debunking Breach Myths: Who is Stealing Your Data?'. Trend Micro, Simply Security, 1 Oct 2015. Accessed Jul 2016. https://blog.trendmicro.com/debunking-breach-myths-who-is-stealing-your-data/.
5. Seals, Tara. 'Insider threats responsible for 43% of data breaches'. InfoSecurity, 25 Sep 2015. Accessed Jul 2016. www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/.
6. 'Network security – are businesses meeting the challenge?'. Hewlett Packard Enterprise Solutions, 19 Sep 2014. Accessed Jul 2016. www.slideshare.net/HPESoftwareSolutions/hp-networksecuritysurveyresults.

EVENTS

6–7 September 2016
CyberTech Singapore
Singapore
http://cybertechsingapore.com/

7–9 September 2016
International Cyber Security & Intelligence Conference
Ontario, Canada
https://icsic.ocmtontario.ca/

14–16 September 2016
44Con
London, UK
www.44con.com

19–20 September 2016
Information Security Network
Reading, UK
https://thenetwork-group.com/information-security-network/

21 September 2016
New York Cyber Security Summit
New York, USA
http://cybersummitusa.com/new-york-2016/

26–27 September 2016
CyberSec: European Cyber Security Forum
Krakow, Poland
http://cybersecforum.eu/en/

27–28 September 2016
Industrial Control Cyber Security Europe
London, UK
https://industrialcontrolsecurityeurope.com/

28–30 September 2016
SCADA & Cyber Security for Power & Utilities Industry
Berlin, Germany
http://bit.ly/29hlbuy