BAE SYSTEMS

Three tactics for tackling insider threats

Executive summary

Mark Rayner
Head of Financial Services Consulting, BAE Systems

It's easy to think that the major threats to your business are purely external – competitors, unforeseen events, civil disruptions and so on. These are genuine risks that any organization – insurers or otherwise – should be aware of. It often pays to look closer to home.

In this Insurance Insights report Mark Rayner, Head of Financial Services Consulting at BAE Systems, looks at the difficulties of tackling insider threats – and explains three things insurers can do to protect themselves.

The damage caused by insiders can be catastrophic – and by one measure, the number of insider attacks outnumbers external raids. In 2017, an employee at a leading private healthcare provider removed personal information relating to 547,000 customers. This was far from an isolated incident – the Information Security Forum has estimated that insiders are responsible for 54 per cent of data breaches. But it's not just data at risk. One staffer at a well-known automotive and energy company in Palo Alto, who reportedly felt overlooked for a promotion, made unauthorized changes to his employers Manufacturing Operating System.

Although we should be pleased such attacks came to light, it is clear that the insider threat has taken firmer root on the business landscape. But it doesn't have to be this way.

54%
of data breaches are committed by insiders
- Information Security Forum

An intelligence-led approach

There are many reasons why organizations are facing a proliferation of insider threats. Although external attackers typically have to penetrate a complex set of defenses, there is little to stop internal attackers from turning their plans into reality. There is also increasing awareness of the value of corporate assets and an abundance of digital tools to help convert them into cash – USB sticks, Bluetooth file transfer and smart personal devices all spring to mind.

And as we have previously illustrated in our report, The Unusual Suspects, internal threats come in many guises: the disgruntled office worker, the blackmail victim in Accounts, the spy, the well-meaning innocent, or the small supplier with trusted access to your network. This makes the Insider one of the hardest suspects to anticipate and defend against.

However, organizations should by no means sit back and meekly await the inevitable attack from disgruntled employees. On the contrary, we think it's time to be proactive and adopt an intelligence-led approach, focused on three major workstreams.

Firstly, **risk.** Insurers – and any other organization – need to understand what they are protecting, from whom and in which scenarios. The key element here is to focus on the critical assets and highly privileged users. Identifying these two groups gives biggest return on investment, but a targeted approach also mitigates concerns over mass data collection. This doesn't happen overnight, but it can be done. Identifying those individuals and groups who can access or influence an organization's critical assets is a good starting point. Of equal importance is highlighting those areas that have the greatest feasibility for an attacker – start with where is most vulnerable and work back from there.

2

Secondly, **policy and governance.** Insurers need to be clear on what they are willing and able to do to protect against insiders.

Due to the sensitivity, this is best tackled with a dedicated Insider Threat Management function with support from a broad range of stakeholders such as HR, Security, Legal, Risk, IT and Procurement for third parties. It also requires ongoing communications and awareness with employees. Organizations need to take this step by step – identifying key stakeholders, implementing the necessary people and process changes and then working with colleagues in internal communications and others to raise awareness and monitor performance.

3

And thirdly: **technical.** Insurers need to put technical and intelligence capabilities in place to deliver the necessary security. Traditional log sources, such as network access and Data Loss Prevention (DLP) logs and building access records, and non-technical sources such as employee performance records can be used to develop a set of risk indicators.

Crucially, insurers also need to ensure they have robust playbooks and response processes in place to triage and investigate alerts. Such operational priorities will, inevitably, take some time to become embedded into an organization's operations but, nonetheless, their importance should not be underestimated.

Winning over the sceptics

However valid this approach may be, expect opposition from colleagues looking outward for threats and opportunities. Do they really need to re-focus their attention on internal issues? Well, yes – not least because, aside from the criminal damage such attacks do, there can also be a huge reputational impact. Here's how.

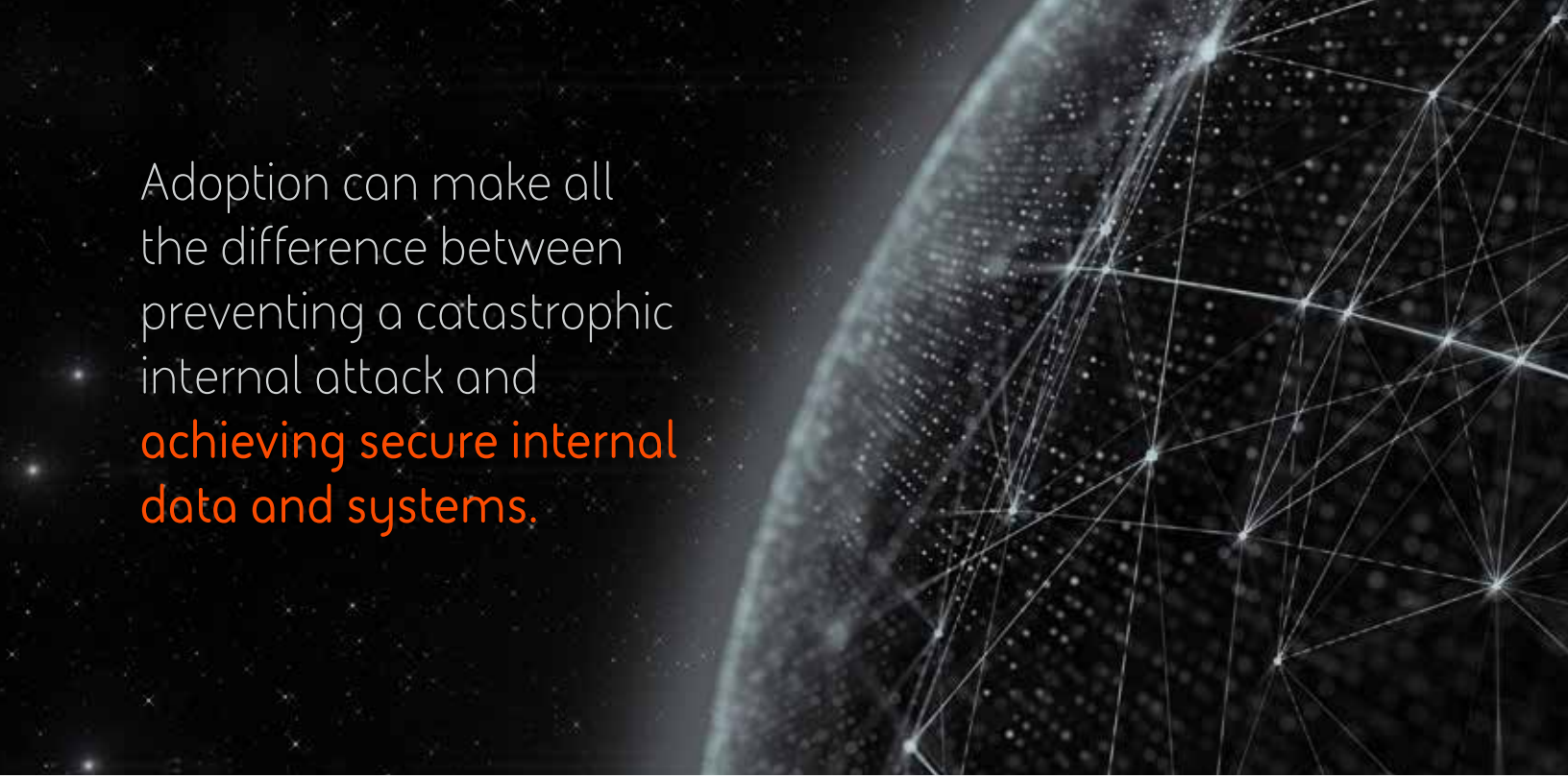
Terminology might be a challenge – "The 'Insider Threat' brand isn't compatible with our culture" is likely to be a common refrain. When this crops up, employees need to be educated on the risks that insiders represent using examples from other industries. Insurers should also consider the deterrent value of having a formal Insider Threat program.

Employees, too, are likely to be somewhat upset by any notion they are no longer trusted. But complaints about management failing to demonstrate trust, or even behaving like Big Brother can be rebutted by reinforcing the need to protect critical assets from accidental as well as malicious attacks. Employees need to understand the governance controls, as well as the involvement of Legal and HR.

Speaking of **HR,** it's important to ensure that background checks are sufficient. It's vital that HR understands why ongoing monitoring is so important in detecting changes that standard checks miss. Tailoring background checks to roles is worth considering.

IT and Security teams are also likely to raise their concerns by pointing to the fact that they already monitor network use. Yes, they do, but understanding critical assets, high risk users and key processes will help improve detection and reduce false positives – helping them in the long run.

And finally, **internal auditors** may either complain about a lack of resources or cite the fact that the company already complies with all the relevant regulation. I'm sure it does but here you can make the case for a risk-led approach, enabling the business to make informed decisions on where and when to invest its precious resources.



Insuring the insurers

Such ideas are clearly suggestions that can be tailored to the individual challenges facing each insurer, large or small. But their adoption can make all the difference between preventing a catastrophic internal attack and achieving secure internal data and systems.

For example, some of the more advanced insurers are using HR data in their fraud detection models to identify cases of collusion – such as where a claims handler re-opens an old claim and adds their personal contacts as fictitious passengers. This is a perfectly valid approach but risks focusing only on the fraudulent claims and missing other vectors including loss of customer data. It should really be part of, not instead of, a broader Insider Program.

Insurers are rightly quick to stress the value of their product to both individuals and customers. Here, though, they need to adopt similar practices themselves in order to guard against this burgeoning risk.

There's no time to waste.

Profile

Mark Rayner

Head of Consulting, Financial Services at BAE Systems

Mark Rayner leads the Consulting Practice within the Financial Services division of BAE Systems Applied Intelligence. He helps banks, insurers and other financial services clients get the most value from the information they hold whilst also protecting themselves from internal and external threats.

Mark specializes in transformation and working with multi-disciplinary teams to mitigate cyber risk, deliver business change and leverage data to transform operations. His experience spans policy and governance, risk and control assessments, data classification and management, business intelligence and analytics.

How we can help

Reducing risks

Insurers must identify their critical assets most prone to insider threat, understand the potential threat scenarios and assess those communities and users most likely to access or influence such assets. We can bring clarity to this complex threat landscape.

Boosting policy and governance

Identifying key stakeholders and defining their roles and responsibilities is a difficult and delicate task. We can help insurers establish a dedicated Insider Threat Management function with the appropriate governance and process framework to make this operational. It's also vital to establish regular communication, training and education to raise awareness and monitor performance of the function.

Technical injection

Insurers require bespoke technical and intelligence capabilities to underpin the necessary security. We can define and embed the business processes necessary to establish a clear baseline and set of controls to manage and monitor the insider threat. We can also help collect and analyse data across the organization to identify emerging levels of risk, and prepare investigation and response processes to respond to insider threats as they arise.

For more information go to: www.baesystems.com/insuranceinsights

Contact us

E: learn@baesystems.com
W: baesystems.com/insuranceinsights

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

linkedin.com/company/baesystemsai twitter.com/baesystems_ai

BAE SYSTEMS