USING DIGITAL FORENSIC WORKFLOWS TO ADDRESS INSIDER THREATS WITH PRIVACY-CENTRIC ACTIVITY MONITORING

EXECUTIVE SUMMARY

The term "insider threat" covers a broad range of malicious or negligent activities conducted by employees, contractors and other organizational insiders. Instances of malicious insider threats are growing; 43% of data breaches that involved an insider were the result of abuse or malicious intent, as of 2020.

The risks posed by insider threats include data exfiltration, workplace bullying or harassment, market abuse and the misuse of client data. These can lead to:

- **Financial risk.** Criminal and malicious insiders cost their companies an average of $756,760 per incident in 2019.
- **Reputational risk.** Companies that suffer from high-profile cases of insider data theft, fraud, bullying and the like suffer reputational damage. This damage can affect customers, who may be unwilling to trust the company again with their data, and employees, who may leave to work for a more reputable organization.

The COVID pandemic has thrust the issue of insider threats to the top of the corporate agenda. For some, home working reduced visibility of workers and created fear and uncertainty in the workforce. Now, the pandemic is giving rise to the concern of extensive and prolonged employee turnover, and many people may be tempted to take data with them when they switch jobs

There is also evidence that home working has shifted workplace bullying and harassment online. According to one survey, nearly half of women (45%) who had been sexually harassed said they had experienced harassment online through sexual messages, cyber harassment and sexual calls; almost a quarter said incidents had increased or escalated since they moved to home working.

Government agencies and professional services organizations are starting to advise businesses on the controls and processes they need to put in place to mitigate the insider threat. The need for effective oversight and activity monitoring is a recurring theme. Concurrently, organizations are investing in technologies that can monitor activity undertaken on the computers allocated to employees in response to specific circumstances.

A key challenge for employers will therefore be to find a technology that balances the need to identify and stop potential criminal, malicious or negligent acts by 'bad apple' employees while respecting the privacy of the law-abiding workers who form most of the company.

We must stop thinking about monitoring in terms of individuals. Rather, companies looking to identify and stop insider threats should focus on *activities* that could harm them, their employees or their customers, leveraging three core components: data, rules and automation.

Taking a privacy-first approach means employees are at no point being actively monitored. Rather, unusual endpoint activity that breaks one of the rules simply alerts digital forensic teams that potentially malicious activity is underway and captures potential evidence for further review.

Professional services firm Deloitte has created a proactive digital forensic workflow known as DFIT (Digital Forensic Insider Threat) to help manage this issue. This workflow allows practitioners to identify threats and preserve forensic artifacts for further review and analysis. Using Nuix Adaptive Security, any unusual endpoint activity that breaks pre-written rules alerts the digital forensic investigator that potentially malicious or negligent activity is underway and captures associated evidence for further review.

Deloitte's DFIT workflow is an example of leading innovation. Leveraging Nuix Adaptive Security as part of any risk management or insider threat program reduces the risk of a serious data compromise or compliance violation, allowing organizations to make intelligence-led decisions that prevent crises.

INSIDER THREATS: THE STATE OF PLAY

A review of literature on the topic of insider threats reveals that companies need to take a data-centric approach focused on end-user activity, rather than monitoring individuals. This requires digital forensic workflows that leverage technology at scale to identify threats as they develop and preserve potential evidence for further investigation and analysis.

INSIDER THREATS DEFINED

According to Deloitte, an insider "can be an employee, contractor or vendor who commits a malicious, complacent or ignorant act using their trusted and verified access."[1]

Public debate on the topic of insider threats often focuses on external actors using compromised credentials or social engineering to gain access to a corporate network.[2] However, the true definition of insider threats is much broader and includes:

- **Data exfiltration by exiting employees.** At least 63% of employees admit to taking data with them to a new job.[3]
- **Workplace bullying and harassment.** Nearly 94% of workers say they have been bullied in the workplace.[4]
- **Misuse of customer data.** A former engineer for Amazon Web Services accessed more than 100 million customer accounts and credit card applications from AWS customer Capital One.[5]
- **Being bribed or coerced by cybercriminals to run malware, expose customers' personally identifiable information (PII) etc.** An engineer at carmaker Tesla was approached by a Russia-based ransomware group, which offered him $1 million to execute ransomware on his work computer.[6]

The threat posed by malicious insiders is growing. Research from Forrester shows malicious insiders accounted for just under half (48%) of internal data breaches in 2015 but this number had jumped to 65% by 2018 before easing back to 61% in 2020.[7]

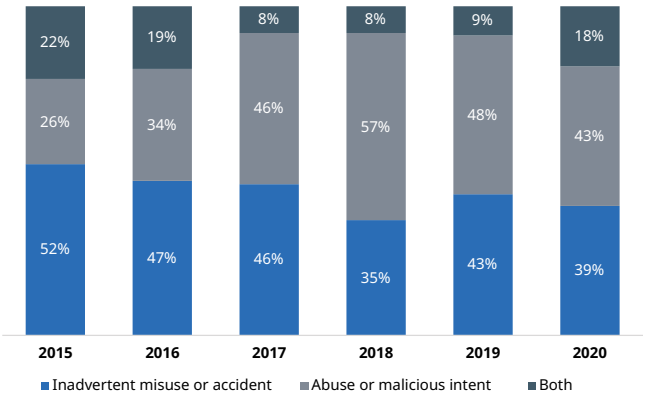

Figure 1: Source of internal attacks. Source: Forrester Research[8]

Employees act maliciously for many reasons, including a sense of financial insecurity, entitlement, having been wronged or having been passed over for promotion as well as announcement of layoffs, fear of being laid off, conflict with colleagues or ideological beliefs.[9]

The financial damage caused by insider threats can be significant. According to research by IBM, criminal and malicious insiders cost their companies an average of US$756,760 per incident in 2019 (see Figure 2).[10] This sum is comparable to the US$871,686 per incident associated with credential theft.[11] Of the 4,716 incidents included in the IBM study, 1,105 were caused by criminal and malicious insiders.

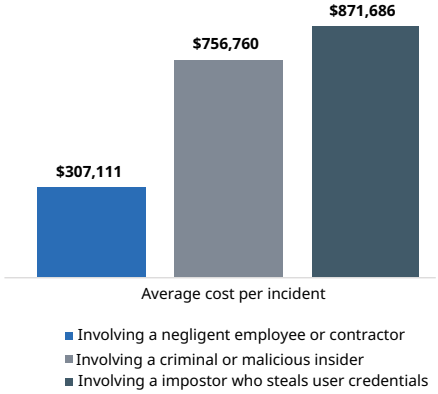

Figure 2: Average cost per insider incident. Source: IBM Security[12]

Regulatory action can form a large proportion of the costs. Under the European Union's General Data Protection Regulation, for example, data protection authorities can impose fines of up to up to €20 million, or 4% of worldwide turnover, for data breaches involving PII.[13] However, the direct costs are only part of the reason business leaders should be concerned.

REPUTATIONAL RISK

Fraud, workplace bullying, data breaches and corporate theft make headlines, in the process creating brand associations that no business wants. More than a third (38%) of IT leaders see reputational damage as the biggest consequence of an insider breach, ahead of financial impact (27%).[14]

A company with a bad reputation, especially regarding workplace bullying and harassment, will struggle to attract and retain talent. Eighty-four percent of job seekers say company reputation is an important factor when applying for a job.[15] Moreover, a study from the Harvard Business Review suggests that a bad reputation equates to a 10% increase in cost per hire.[16]

IMPACT OF THE COVID PANDEMIC

If insider threats were important before COVID, the pandemic has thrust the issue to the top of the corporate agenda, for three key reasons:

1. While the adoption of remote working at scale was necessary to keep businesses operational, it also reduced visibility of workers just as it created fear and uncertainty in the workforce, a mix that Forrester calls "the ideal conditions for insider incidents."[17]
2. The pandemic has ushered in a prolonged period of widespread employee turnover dubbed the "great resignation." According to one survey, up to 40% of people are currently considering changing jobs.[18] As already mentioned, at least 63% of employees own up to taking data with them to a new job, making the great resignation a significant threat to businesses.[19]
3. While people have been working from home, workplace bullying and harassment have shifted online. According to a report by the Fawcett Society, a charity that campaigns for gender equality, nearly half of women who experienced workplace harassment did so online in the form of sexual messages, cyber harassment and sexual calls.[20] Moreover, nearly a quarter of respondents said incidents increased or escalated following the move to home working.[21]

OVERSIGHT AND MONITORING

Across all industries, government agencies and professional services organizations are starting to advise businesses on the controls and processes they need to put in place to mitigate the insider threat. The need for effective oversight and monitoring is a recurring theme.[22,23]

For instance, a 2020 report by Canada's Office of the Privacy Commissioner (OPC) investigation report says the "human factor is the weakest link when it comes to information protection in a technological environment."[24]

OPC cites oversight and monitoring as key tools in the battle against insider threats. These include "technological measures such as active information system monitoring, a user and entity behavior analytics solution, logging, and a data loss prevention solution … to detect suspicious uses of resources and employees' potential non-compliance with the organization's directives and policies and to detect and prevent the exfiltration of sensitive data."[25]

MANAGING INSIDER THREATS

Given the scale of the financial, regulatory and reputational risk, it is little surprise that many organizations are taking action to mitigate insider threats. Market Research Future estimates organizations worldwide will spend $6.84 billion on employee activity monitoring solutions from 2021 to 2028.[26]

Employee activity monitoring technologies enable businesses to protect their own data beyond the traditional physical workplace. An increasing number of businesses are adopting such technologies as home working becomes part of business as usual. According to one survey, 20% of UK organizations are already using, or plan to introduce, software to monitor employees who are working from home.[27]

Forensic technologies – such as those based on artificial intelligence (AI) models, automation and workflows – can help detect and stop insider threats and manage the risk of regulatory non-compliance. Tools that alert organizations to suspicious activity can be implemented as part of a remediation process following an investigation.

Adopting such technology allows for a more cost-efficient and timelier conclusion of internal investigations, regulatory inquiries and litigation.

PRIVACY CONCERNS

While a growing number of businesses see the merits of oversight and activity monitoring tools, they can also cause concern for employees, trade unions and privacy advocates. One UK study found that by the end of 2021 32% of workers were being monitored in some form by employers, up from 24% in April 2020.[28] Prospect, a trade union for professionals working in technology, engineering, management and the civil service, is now calling for measures to protect employees from "intrusive monitoring".[29]

Considering such concerns, it is important for business leaders to have a legally defensible and reasoned position why they need to deploy monitoring solutions. As demonstrated by the UK Trades Union Congress, different types of monitoring are acceptable to workers to varying degrees.[32] For instance, monitoring company assets appears to be broadly acceptable, surveillance that focuses on individuals is considerably less so.[33]

Should employers be allowed to use webcams to monitor remote workers?

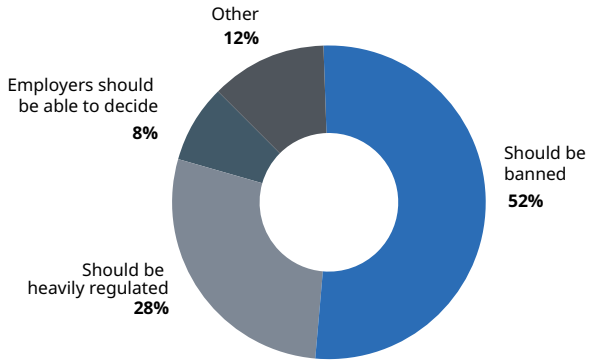

Figure 3: Employee attitudes to webcam monitoring. Source: Prospect[30]

THE THREAT LANDSCAPE: DELOITTE'S TAKE

As the world emerges from the COVID-19 pandemic, one key change to our working patterns looks set to stay: the widespread adoption of remote working.

According to the Chartered Institute of Management, 80% of UK firms had adopted some form of hybrid working by mid-2021.[34] For some, this has meant an uptick in employee productivity and, in turn, company results. This is likely to increase employee wellbeing stemming from the increased flexibility people now have over their work lives, although for some the lack of an office can be isolating.

With these benefits, however, come a new set of problems that employers need to deal with. If an employee is working in several geographically separate environments, on different devices (a bring-your-own device for example) and on different matters, a wide variety of data needs to be made available to them to do their jobs. This data can come in many forms, such as USB drives, email and document management platforms. This increased availability and quantity of data can be a huge risk for a business. Can we be sure that the access to this data is genuine?

There is also a challenge around an employee physically traveling between working locations. Before the pandemic, an office worker would securely stow away their laptop at work, or perhaps take it home on rare occasions. Nowadays, someone could be traveling to a new location daily, which increases the risk of "shoulder surfing" or leaving a laptop on a train or in a café.

We have had repeated success with our Digital Forensic Insider Threat (DFIT) proposition, which utilizes Nuix Adaptive Security, in helping our clients deal with some of the issues mentioned above and the insider threat as a whole.

One of our key experiences was helping a major financial institution ensure it had sufficient safeguards for its workforce to move to a hybrid working setup. We worked closely with stakeholders at the company, understood its areas of risk and implemented rules to inform us of actions that could be indicative of insider threat. The business saw the benefit that DFIT brought to them and introduced it into their long-term insider threat strategy

— **Richard Williams**, *Partner, Deloitte UK*

CONCLUSIONS

A clear picture has emerged: insider threats are rapidly increasing in number and in the financial and reputational damage they cause. Moreover, regulators and the legal sector are shining a spotlight on the tools and processes organizations are putting in place to mitigate these threats.

Dealing with this problem delivers benefits to a broad range of stakeholders:

- **Businesses leaders** and owners stand to gain from limiting theft, data exfiltration and fraud committed by employees. In addition to limiting financial losses and regulatory penalties, their organizations can build a strong brand that customers trust.
- **Customers and employees** benefit because they know that their data is protected. Headline-grabbing instances of credit card numbers, emails and other sensitive data being exposed have made consumers more aware of the risks they take when they hand over their personal information. The data on this subject speaks for itself: 81% of consumers say they would stop engaging with a brand following a data breach; 63% believe a company is always responsible for protecting their data.[35]
- **Employees** benefit through a workplace less open to bullying and harassment. What's more, since 76% of job seekers and employees say a diverse workforce is an important factor when evaluating companies and job offers, creating a better environment for employees helps businesses attract the talent they need.[36]

There is clearly a market need for oversight and activity-monitoring tools that can help address insider threats and proactively capture digital forensic artifacts to identify and alert an organization of potentially nefarious activities. However, a key challenge for employers will be to find a technology and a scalable and defensible workflow that balances the need to identify and stop criminal, malicious or negligent acts, while respecting the privacy of the law-abiding workers that form most of a company.

RECOMMENDATIONS

We must stop thinking about monitoring in terms of individuals. Rather, companies looking to crack down on insider threats should focus on activity that can harm the organization or its clients.

Deloitte's Digital Forensic Insider Threat (DFIT) workflow is an industry-leading approach. The Deloitte DFIT workflow identifies, collects and preserves potential evidence in real time for further analysis by the digital forensic investigation team. This approach leverages three core components:

- **Data.** When it comes to the digital forensic investigation of potentially malicious activities, data is crucial. Organizations must make efforts to capture all information relevant to an ongoing investigation. To protect employee privacy and save resources, data relating to potential malicious activity must be identified and preserved. This is achieved by focusing purely on the corporate device (endpoint) and any malicious activity involving both corporate and non-corporate data repositories that are flagged by the pre-defined rules and policy controls.
- **Rules.** Understanding what normal endpoint activity looks like enables organizations to establish an adaptable ruleset, which they can use to discover potential employee misconduct and investigate it, quickly and discreetly. The customized rules used in Deloitte's approach trigger the digital forensic workflow; a process that is enabled through AI-derived automation.
- **Automation.** When alerts appear, an automated workflow can triage the threat and capture potentially relevant information as it is happening, mitigating the risk of losing digital evidence. Deloitte employs advance automation technology to ensure rapid and effective activity analysis and data capture.

PRIVACY FIRST

This is an example of a privacy-first approach – employees are at no point being actively monitored. Rather, unusual endpoint activity that breaks one of the rules simply alerts digital forensic teams that potentially malicious activity is underway and captures potential evidence for further review. (This is one of the core features called out in Canada's Office of the Privacy Commissioner's recommendations – see Oversight and Monitoring on page 3). The use cases for rules-based threat monitoring include:

- Identifying when a USB storage device is plugged in and data downloaded onto the device
- Monitoring collaborative communication platforms to alert when keywords associated with workplace bullying are used
- Alerting when an employee copies and pastes a credit card number or other PII into an email or other non-secure location
- Alerting when an employee bulk copies documents outside of typical working hours.

One of the core benefits of Deloitte's DFIT workflow is that it allows digital forensics to become more proactive. Digital forensics has traditionally been a reactive process that plays out only after an event. Here, data is collected from sources including computers, smartphones and remote storage. However, the time delay between the malicious act and data retrieval provides many opportunities for important evidence to be deleted, lost or misplaced. By using forensic practices with the DFIT workflow, organizations can now identify the event , or a pattern of activity that foreshadows the event, in near real time.

The Deloitte DFIT workflow puts smart automation at the heart of threat monitoring. Employees can carry on their work lives safe in the knowledge that they are not being tracked or monitored, while employers can rest assured that activities which trigger an alarm will be monitored and all relevant data will be preserved. This privacy-centric, comprehensive approach to insider threat management will help businesses meet the challenges they face.

NUIX ADAPTIVE SECURITY

Deloitte's DFIT workflow is powered by Nuix Adaptive Security. Nuix Adaptive Security provides an efficient approach to real-time activity monitoring and investigation across endpoints. The powerful, streamlined, confidential and discreet software enables firms to rapidly set up adaptable rulesets to discover and investigate the full range of insider threats.

Deloitte's thorough approach to defining rulesets delivers a truly privacy-first approach where rules are not set up against specific individuals and data is only collected once a rule is triggered. Additionally, Deloitte works with clients and their legal teams to tailor the DFIT workflow and Nuix Adaptive Security ruleset to address local legal and regulatory requirements.

In summary, with Nuix Adaptive Security organizations benefit from:

- Adaptable rulesets for specific issues
- Advanced evidence captures (including keystrokes, screen and printer)
- A unified investigation tool (with the data in one place)
- A data privacy-centric workflow.

These features allow security teams to:

- Investigate potentially malicious or negligent activity in minutes rather than days by capturing events on the endpoint and streaming them back for immediate analysis
- Intercept malicious activity before it interrupts business as usual
- Perform fast, targeted evidence collection of live and static data – at scale, in advance or on demand – with digital forensic capabilities that form part of a robust and defensible case
- Change logic rules and adjust response posture on the fly, enabling digital forensic teams to continuously improve their risk management processes and approaches.

Nuix Adaptive Security is available through the Deloitte–Nuix Alliance, which brings together the companies' respective strengths in market-leading global consulting and data processing, analytics and intelligence software in a powerful combination to address clients' eDiscovery, business transformation, governance, forensicinvestigations, incident response and endpoint monitoring needs.

Leveraging Nuix Adaptive Security as part of any risk management or insider threat program reduces the risk of a serious data compromise or compliance violation, allowing organizations to make intelligence-led decisions that prevent crises.

NUIX ADAPTIVE SECURITY: DELOITTE'S TAKE

Nuix Adaptive Security was initially positioned for a niche sector however we identified a wider application for its use. Over the past two years we've integrated Nuix Adaptive Security into our proactive digital forensic workflow which we call – DFIT, Digital Forensic Insider Threat.

Digital forensic techniques have been traditionally deployed as part of investigations or litigation – but sometimes weeks or months after an alleged event or incident has occurred. This can create obvious challenges. Nuix Adaptive Security now gives us an advantage allowing us to identify risks or concerns in near to or in real-time.

Nuix Adaptive Security is allowing us to use digital forensic techniques as part of traditional investigation but in a proactive stance. This ability allows us to establish facts in a fast-moving investigation involving issues such as data exfiltration, bullying and harassment claims and policy breaches. We can now do this in a way that preserves the confidentiality of those involved as well as the integrity of the data examined.

— **PAUL TAYLOR**, *National Lead Partner for Digital Forensic, Deloitte Australia*

ABOUT THE AUTHORS

PAUL SLATER
Director Government, EMEA

Paul has over 25 years of experience in digital forensics and investigations, having worked in law enforcement, corporate and government organizations including the UK's Serious Fraud Office and two of the Big 4 advisory firms. As a thought leader and the investigations subject matter expert, Paul advises customers on forensic technology solutions including electronic disclosure, litigation readiness, data compromise and forensic data analysis. He has helped shape Nuix's investigations products, solutions and messages, and been instrumental to customer success stories.

NEIL THOMAS
Director, Advisory & Service Providers EMEA

Neil creates cost-effective, customized customer solutions using Nuix technology to solve complex problems and help organizations gain value from their data. He started his 25-year career in IT security before transitioning to consulting roles delivering market-leading global payment solutions within regulated markets to help businesses compete internationally. He has held leadership roles at Western Union, Thomas Cook and Prudential.

REFERENCES

1. Adnan Amjad, Mike Gelles, Unmasking insider threats, Deloitte, June 2015
2. Joseph Blankenship et al, Best Practices: Mitigating Insider Threat, Forrester, March 19, 2021
3. Mark Wojtasiak, Your employees are making a run for it, and so is your data, Security Info Watch, December 4, 2021
4. Bryan Robinson, New Study Says Workplace Bullying On Rise: What You Can Do During National Bullying Prevention Month, Forbes, October 11, 2019
5. Blankenship op. cit.
6. Christopher Burgess, Tesla Insider Works with FBI to Turn the Tables on Russia's Million Dollar Attempt to Hijack the Network, ClearanceJobs, August 26, 2020
7. Blankenship op. cit.
8. Ibid
9. Ibid
10. IBM, Cost of Insider Threats: Global Report 2020, April 2020
11. Ibid
12. Ibid
13. itgovernance.co.uk, GDPR Penalties and Fines | What's the Maximum Fine?, retrieved March 15, 2022
14. Luke Irwin, CIOs increasingly concerned about insider threats, GRC eLearning, April 23, 2019
15. Jessica Thiefels, Why Investing in Employer Brand Pays Off, Glassdoor, January 28, 2020
16. Wade Burgess, A Bad Reputation Costs a Company at Least 10% More Per Hire, Harvard Business Review, March 29, 2016
17. Blankenship op. cit.
18. Wojtasiak op. cit.
19. Ibid
20. Molly Mayer et al, Tackling sexual harassment in the workplace: Report on employer actions to prevent and respond to workplace sexual harassment, Fawcett Society, October 2021
21. Ibid
22. US Cybersecurity and Infrastructure Security Agency, Insider Threat Mitigation Guide, November 2020
23. UK Centre for the Protection of National Infrastructure, Monitoring and Assessment, retrieved March 15, 2022
24. Bradley Freedman, Privacy Commissioner Report - Guidance for managing insider threats, Borden Ladner Gervais LLP, February 2, 2021
25. Ibid
26. Market Research Future, Employee Monitoring Solution Market Research Report, February 2021
27. Jonathan Owen, One in five employers monitoring remote workers or planning to do so, poll finds, People Management, November 26,2020
28. Prospect, New protections needed to stop employer surveillance of remote workers, November 5, 2021
29. Ibid
30. Ibid
31. Dan Lucy, Workplace surveillance: one to keep an eye on?, Institute for Employment Studies, October 27 2020
32. Trades Union Congress, I'll be watching you: A report on workplace monitoring, February 2020
33. Lucy op. cit.
34. Chartered Management Institute, What you think about WFH, flexible and hybrid working: the results are in, May 5, 2021
35. Ping Identity, 2019 Consumer Survey: Trust and Accountability in the Era of Data Misuse, December 2020
36. Glassdoor, Glassdoor's Diversity and Inclusion Workplace Survey , September 29, 2020

Nuix (www.nuix.com, ASX:NXL) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849