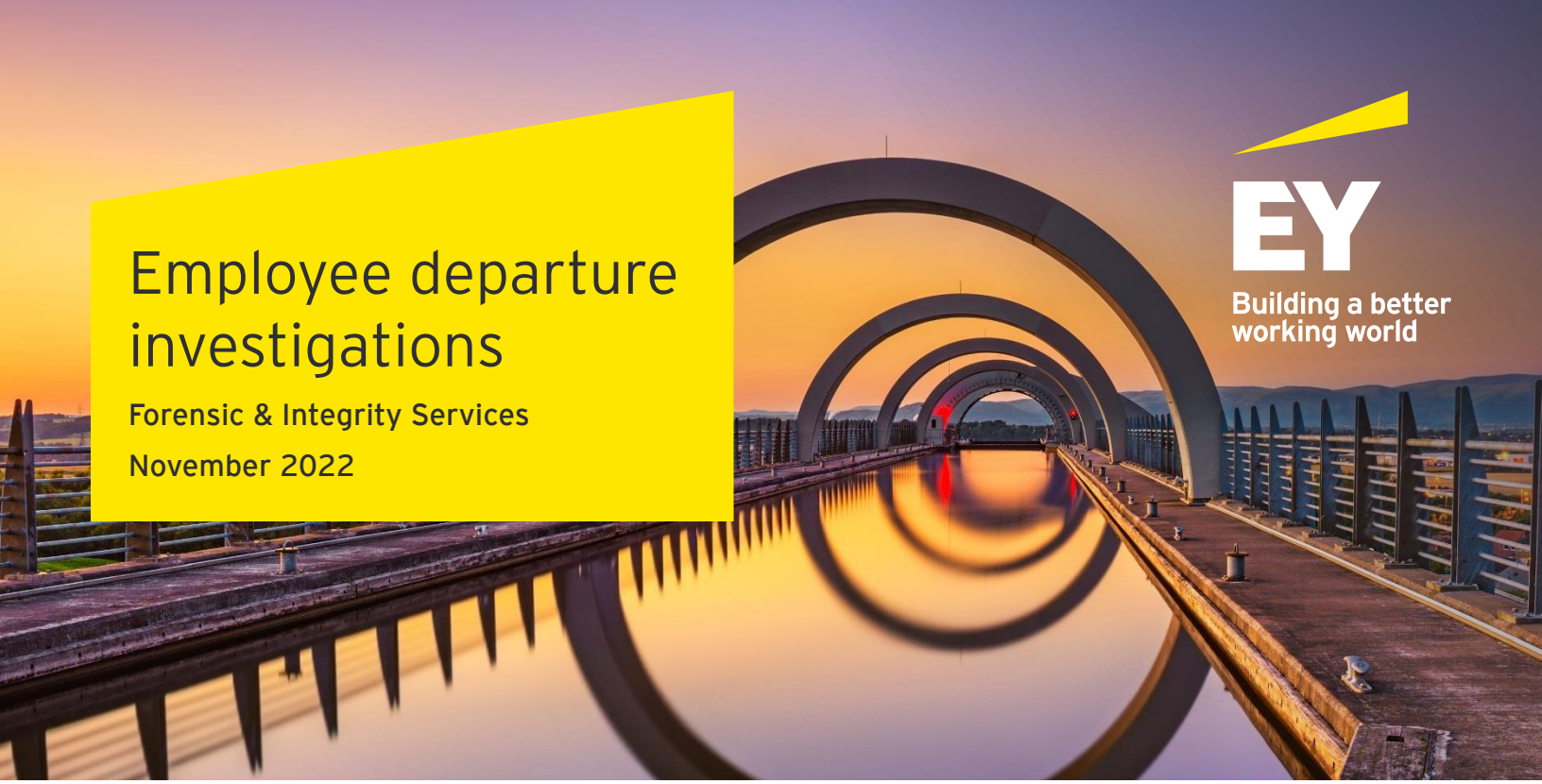


Employee departure investigations

Forensic & Integrity Services

November 2022

EY
Building a better working world

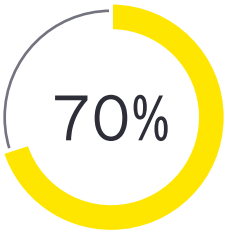
Today's data landscape

Among the biggest threats to companies are their recently departed employees. Former employees can take data with them upon departure through printed documents, sending documents to a personal email or cloud account, messaging about company information or even having access to cloud accounts after their last day.

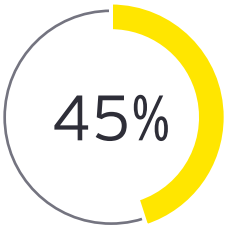
It's not always malicious. The employee might preserve a copy of data they designed or implemented because they believe they have a right to it. If a company allows the employees to use their personal devices to conduct business, a former employee may not realize they are still in possession of company data after their employment.

Despite cautious efforts, inside actors may still be able to take privileged company data with them. Having protocols already in place will help confirm that your company is prepared for any situation involving an employee's departure — while reducing the risk of a former employee disclosing company data to a competitor.

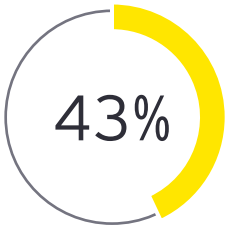
Challenges faced by organizations



of intellectual property theft occurs within the 90 days before an employee's resignation announcement.[1]



of employees download, save or send work-related files before they leave their job.[2]



of data exfiltration instances in 2020 involved business emails forwarded to personal accounts.[3]

1. How to Keep Data Safe When Offboarding Employees (Checklist & Guide) | CurrentWare
2. 41 Insider Threat Statistics You Should Care About | Swiss Cyber Institute
3. U.S. insider threat data exfiltration behaviors 2020 | Statista

Analysis lifecycle

	Pre-collection and analysis	Information gathering	Preservation and preparation for analysis	Analysis and reporting		Follow-up analysis and remediation
	Device preparation	Identify target devices	Preserve target devices	Analysis of data performed	Preliminary reports provided to client	Analysis, remediation, supplemental collections
Forensic procedure	Avoid giving the devices to additional users, and avoid using the device	EY team works with client or counsel teams to determine scope of investigation	Forensic collections of any devices or accounts that were identified in Phase 1	EY team performs analysis on all identified devices and/or accounts, focusing on date range	Review of reports to determine next steps of investigation (e.g., remediation, collection of additional devices)	Final analysis of device(s) and accounts; remediation if privileged documents were identified; perform additional collections if necessary
	1	2	3	4	5	
Typical evidence examples	Leave the device(s) powered off and in a secure location until EY team's collection	Identification of devices and accounts used by target individual and key dates associated with concerns	Forensic collections of any identified devices or accounts (e.g., laptops, media, mobile devices, cloud storage accounts)	Analysis of USB, internet and cloud storage activity, as well as deleted and recently accessed mobile device communications	Reports reviewed to determine the former employee's activities leading up to the departure; if necessary, identify documents for remediation or additional devices to be collected	Perform remediation; return devices as requested; perform investigation on additional devices or accounts if identified during initial investigation

EY Digital Investigations and privacy workflow

Service setup

- Help establish procedures (e.g., drawdown of services, standardized matter initiation process)
- Agree on procedures for case management and investigation handling
- Identify key points of contact for accountability, risk and quality management
- Define responsibilities for discharging legal and regulatory obligations
- Develop HR procedures
- Help determine access to local internal and external legal advice
- Perform a conflict check
- Provide elements of core team with support as necessary
- Handle client contacts in core countries
- Hold continuous touch points and briefings

Mobilization and deployment

- Matter or investigation identified by client
- EY teams to identify local resources and work with client to create response teams
- Coordinate tool selection and utilization
- Confirm tool/technology compatibility
- Deploy appropriate resources to project site(s)
- Dedicated local EY contacts assist

Data collection and analysis

- Perform on-site or off-site data imaging for various types of devices/data sources
- Engage in the appropriate chain-of-custody procedures
- Initiate EY evidence tracking processes
- Securely transfer data to EY forensic lab for preservation or further analysis (or in some instances, to the client or another vendor per client's request)
- Perform digital forensic analysis

Reporting and disposition

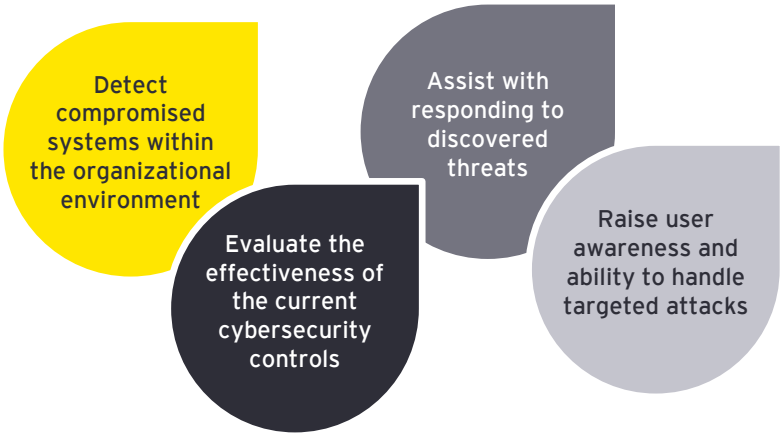
- Agree on next steps with client
- Finalize forensic report and provide to client or outside counsel
- Perform any additional supplemental analysis as requested
- EY teams to maintain data in offline, secured digital forensic labs around the world
- EY teams will retain copies of data for seven years unless otherwise instructed by client

EY resources

EY, client and/or outside counsel resources

The EY approach

We believe that a proactive approach will help your organization respond to complex incidents that may have breached your security. This can help reduce the amount of time a network is exposed, mitigate the damage or data loss that results, and increase the probability of catching the perpetrator.



We start the hunt by understanding the network and systems architecture in place coupled with leveraging cyber threat intelligence to develop a deep understanding of who might be attacking you and why, and, most importantly, how they might do it.

Using a combination of the methods described, we then analyze suspicious activity, assist the organization in responding to it and perform follow-up monitoring to detect anything that remains.

Contact us

Shawn Fohs
US Digital Investigations and Privacy Lead
Managing Director
Ernst & Young LLP
shawn.fohs@ey.com

Joseph Pochron
Senior Manager
US Digital Investigations and Privacy
Ernst & Young LLP
joseph.pochron@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

US SCORE no. 17742-221US

2210-4105658
ED None

ey.com/us/forensics/discovery