mimecast

The Hidden Security Costs of Employee Turnover

And why your offboarding checklist is missing something important

OCTOBER 2022

The hidden cost of turnover

The cost of employee turnover is already high on the agenda of any HR and business leader. And it's no surprise:

The cost of recruiting a new hire, onboarding and training alone can add up to between 50-60% of their salary, according to the SHRM. Add in lost productivity, the new employee ramp time, knowledge loss and morale impacts, and that range moves up to 90-200% of salary.[1]

But as bad as these numbers look, there's a hidden cost of employee turnover that could be many, many times higher—for a single incident. That's the cost to the business when a departing employee takes the company's intellectual property (IP) with them.

Terms like 'data loss' and 'IP' may seem quite abstract. But the impact becomes painfully real when you start to consider the kinds of files that walk out (or are sent out) of businesses every day. Things like:

- Source code
- Product designs
- Customer lists
- Marketing plans
- Employee records
- Proprietary methodologies

Strategic assets like these cost a lot of time, money and effort to create. And they hold significant value to the business. Losing them can irreparably damage competitive advantage.

Instead of looking the other way and making insider threat 'someone else's problem', enlightened HR leaders are working closely with CISOs and data security teams to close the gaps that allow data to leave.

Against the general trend, they're actively driving down this hidden cost of employee turnover through a coordinated, strategic effort to minimize the risk of data loss to the business. And it's working.

The cost of malicious insider attacks has increased by 15 percent year on year and is now an average of US $1.6 million annually for an organization.

- Accenture, Cost of Cyber Security 2019 report

50% of information security leaders said employee actions caused a data breach in their companies in the last 18 months.

- 2019 Code42 Data Exposure Report

The typical data breach now costs a company $3.86M, up 6.4% from 2017.

- Ponemon Institute, Cost of a Data Breach survey, 2018

Insider threat: why it's a growing threat (and cost) for HR

Insider threat is growing fast, driven by societal and technology dynamics, including:

- **More employees switching jobs** – More employees changed jobs in 2018 than ever before – 40 Million in the US, according to the Bureau of Labor Statistics. [2]
- **The explosion in cloud collaboration and file sharing platforms** – Code42's 2019 Data Exposure Report showed that 8 of the top 10 data exfiltration vectors are cloud-based. [3]
- **A more distributed workforce** – "New work arrangements—greater use of contractors and remote work—make the need for employee training more urgent" according to the Accenture Cost of Cyber Security 2019 report.

This collision of the new, open, collaborative work culture with an increasingly mobile, distributed workforce creates the perfect conditions for significant data loss through insider threat.

> "Combined with the expanding threat landscape, organizations are seeing a steady rise in the number of security breaches."
>
> – Accenture Cost of Cyber Security 2019 report

The costs of a data loss incident can hit the company from many different angles, including things like:

- Fines, lawsuits and reputation loss
- Lost product advantage
- Compromised go-to-market programs
- Brand trust and morale damage

These are the kinds of things that move share prices. And for any HR leader eager to prove the value of HR to the business, this is a high-profile, high-impact issue.

Sharing is good…but creates risk

Every HR leader recognizes the real benefits of an open, collaborative work culture and understands the role of software and cloud services in making it happen.

> "73% of CHROs believe that significantly changing the technologies employees use for work will drive engagement & enable growth."
>
> – Corporate Executive Board's Future of Work 2019 study

But not many understand the real risks created by such an open culture. CISOs and security teams do.

> "89% of information security leaders believe the fast paced cultural model of their business puts their company at greater risk of data security threats"
>
> – 2019 Code42 Data Exposure Report

This gap between what HR and security leaders know is closing fast. We need to ensure that we preserve our collaborative, open culture and, at the same time, mitigate risk.

"Ex-Google and Uber engineer charged with trade secret theft."

"Coca-Cola hit with insider breach, 8,000 affected"

"SunTrust Ex-Employee May Have Stolen Data on 1.5 Million Bank Clients"

"Former Hershey Exec Steals Trade Secrets"

"IRS employee steals identities to go on a 2-year spending spree"

"Data breach affects 45,000 patients including San Francisco Department of Public Health records"

Securing your collaboration culture

“To embed cybersecurity into the fabric of the organization and be effective against any insider threats, organizations must bring together human resources, learning and development, legal and IT teams to work closely with the security office and business units.”

– Accenture Cost of Cyber Security 2019 report

We’re all in this together.

Driving down the cost of employee turnover caused by insider threat comes down to a collaborative effort between the security, HR and IT departments as well as line-of-business leaders.

While HR ‘owns’ the cost of employee turnover, insider threat can’t be owned by any single department. It’s a shared responsibility. In part, it’s an education job:

“72% of employees believe their work is their property” and “60% of employees admit to taking data from job to job”

– 2019 Code42 Data Exposure Report

The 90-day lookback:

A new addition to your offboarding process

When thinking about controlling the cost of IP loss, it helps to start at the end: the day an employee leaves the business.

Every company has some kind of offboarding process to protect both the business and the departing employee. Since offboarding needs to cover so many different things, many companies use a checklist (you can find our IG Checklist for Security Employee Offboarding here).

If offboarding checklists cover security at all, they usually focus on physical security: returning laptops, key cards and revoking systems access (including alerting process and system owners to initiate their own procedures).

But the offboarding process is also a critical opportunity to identify and address any data breaches. Departing employee data breaches mostly occur in the weeks before an employee announces his or her departure—as well as the days before their actual final day. It makes sense to review data movement during this period to look for suspicious behaviors, including:

- A spike in the amount of data transfers
- Data movements on weekends or after hours
- Changes in the access permissions for cloud files
- Emailing files to personal or non-company addresses
- Accessing files from a source not normally accessed

This kind of activity doesn’t necessarily indicate bad intent. But it does signal the need to ask some questions and do some investigating.

The 90-day lookback

The 90-day lookback is a powerful technique for assessing the risk of data loss for each departing employee. But to do it, you need a way to monitor all data movements—including the ability to see inside files (instead of judging sensitivity based on file names alone).

This kind of insider threat detection is very different from traditional data loss prevention solutions that attempt to block access to sensitive files (DLP techniques tend to severely inhibit the open collaboration that so many companies are striving for).

The idea is to:

- Let people work how they like to work
- Assume positive intent for most employees
- Educate everyone on the importance of data security
- Monitor data movements to spot anomalies

The response

If the 90-day lookback surfaces suspicious data movements, both HR and the security team need to be notified. The first response is almost always to talk to the employee involved. In most cases, there's a good explanation for the anomalies. But when there is real cause for concern, the whole team will be relieved to have prevented a costly, damaging data breach.

That's what the last day of employment (and the preceding weeks) should look like. Now let's rewind to day one: the day an employee is hired.

Day one: Onboarding

Driving down the cost and IP risk associated with employee turnover starts when the employee joins.

Every onboarding process should include rigorous, comprehensive training on the essentials of insider data security, including things like:

- The cost of data loss
- The policies and processes that support data security
- The systems used to monitor data movements
- The law and the company's expectations
- The potential consequences of a breach

Specific reviews of best-practice use of cloud and collaboration tools must be a part of this. If people learn how to safely access, store and share files, they'll default to that safe behavior. If they don't, they won't.

In short, it's imperative to upgrade your onboarding to align it with your existing security policies and messages.

Keep the conversation going

Of course, reducing insider threat can never be a 'one and done' conversation.

Instead, make it an ongoing theme throughout the employee lifecycle. Use a variety of communications channels, including:

- Regular eSecurity training – in your company portal, collaboration space, or eLeaning platform.
- Computer log-on messages — a consistent reminder of responsibilites each time an employee starts their work.
- All-hands communications – including meetings, videos and email.
- Group workshops – showing small teams what best practice looks like.

> "Training employees to think and act with security in mind is the most underfunded activity in cybersecurity budgets."
>
> – Accenture Cost of Cyber Security 2019 report

Signalling trust

You want to create policies that show you trust your employees instead of policies designed around the few who may bemalicious. Show that you do trust people and are working towards a positive work culture for the majority. And be transparent about the security that's in place. You'd much rather avoid problems than catch people!

Conclusion

Expose the hidden cost of employee turnover

Every HR leader understands the cost of employee turnover. Now, they're increasingly prioritizing the less obvious cost: data loss through insider threat.

Today, enlightened HR leaders are working closely with security and IT leaders to better understand insider threat and minimize the risk.

Get it wrong and you expose the business to significant potential losses that are entirely avoidable.

Get it right and you enable the open, collaborative work culture that every company wants—while increasing security.

This is an important new sphere of influence—and source of impact— for HR and line of business leaders.

And the tools and techniques needed to address it are available, and proven across every kind of company and industry.

> "Counteracting internal threats is still one of the biggest challenges facing business leaders today."
>
> – Accenture Cost of Cyber Security 2019 report

Sources

[1] Cascio, W.F. 2006. Managing Human Resources: Productivity, Quality of Work Life, Profits (7th ed.). Burr Ridge, IL: Irwin/ McGraw-Hill. Mitchell, T.R., Holtom, B.C., & Lee, T.W. 2001.

How to keep your best employees: Developing an effective retention policy. Academy of Management Executive, 15, 96-108

[2] US Bureau of Labor Statistics, Monthly Labor Review, July, 2019

[3] Code42 Data Exposure Report, 2019

About Mimecast

Secure human risk with a unified platform.

Mimecast's connected human risk management platform prevents sophisticated threats that target human error. By gaining visibility into human risk across your collaboration landscapes you can protect your organization, safeguard critical data, and actively engage employees to reduce risk and enhance productivity.