5 Steps to Prove Incydr's Value and Gain the Executive Support You Need

It's time to renew Mimecast Incydr, but you're not sure if you have the executive support you need to secure budget and buy-in. Incydr protects your company's crown jewels, all without slowing down collaboration. You know this, but does the executive team?

Here are 5 steps to prove to the executive team and board that Incydr is the tool you need to meet the bottom line and protect data.

1. Make the Risk Real

First things first, make the risk real. Show them statistics of how much a data breach costs a company, give real life examples of data breaches, determine how much your company's IP is worth - put a number on it. Remember, the risk doesn't stop at the obvious financial costs a breach has on a company. You also have to consider potential regulatory, public relations, legal, and intangible costs associated with the company's reputation.

Real life examples

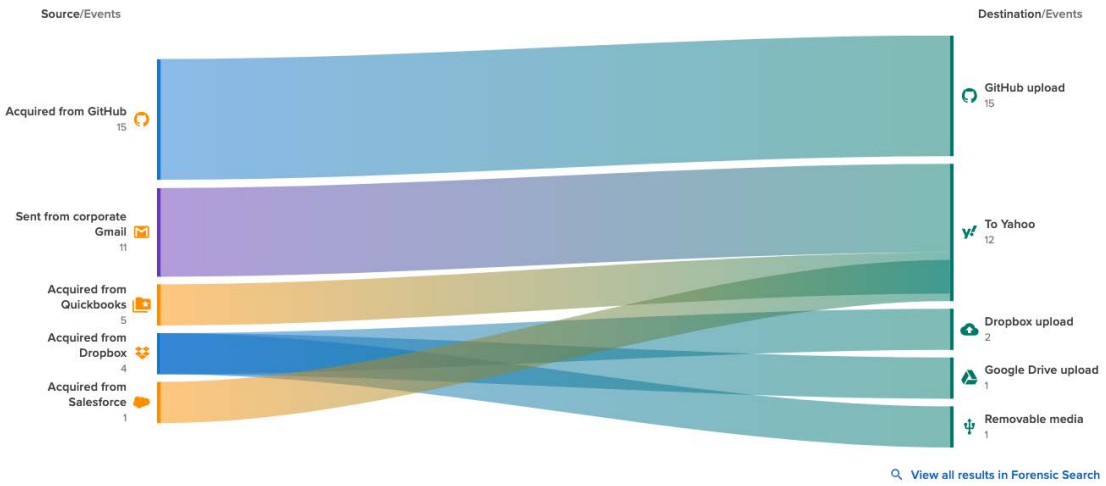
- Ex-Google engineer charged with stealing AI trade secrets while working with Chinese companies
- Medical Center Fined $4.75M in Insider ID Theft Incident
- Over 8 million Cash App users possibly affected by data breach from a former employee

Resources

- Data Exposure Report 2024
  - 85% of cybersecurity leaders expect data loss from insider events to increase in the next 12 months.
  - Insider-driven data exposure, loss, leak, and theft events can have vast financial repercussions, with cybersecurity leaders estimating that a single event would cost their company $15 million, on average.
- Total Economic Impact (TEI) of Code42 Incydr: A Forrester Study
  - The composite organization experienced a 40% reduction in loss per major data exfiltration incident, avoiding $686,000 in losses due to data exfiltration over three years.

2. Report On (and Visualize) the Results that Matter Most

Which metrics and/or reports are most important to your executive team and board? Is it the overall reduction in the number of alerts? Is it seeing fewer investigations? Or understanding how data is moving? Once you know what matters most to them, you can easily pull reports from the dashboards in Incydr. The data visualizations in Incydr–like the graphic below showing how your data moves–will also help the executive team and board truly understand how Incydr tracks how your data moves and how risky that movement may be.



3. Identify Key Use Cases

While this may seem simple, defining the use cases for the tools in your security stack is extremely helpful for consolidating and effectively securing support from outside your team.

For Incydr, take the time to think about the following:

- What kind of data are you most concerned with protecting?
- Which vectors do you view as most risky in your environment?
- Which group of employees would you consider most high risk?
- Do you understand all the capabilities of Incydr and how they can help solve for your needs?
- Have you automated security workflows where possible?

The clearer you can be about the needs Incydr helps you solve for, the more likely your executive team will understand the value and provide support. It will also help you ensure your team uses all your security tools to their fullest potential and that you're getting the most value.

4. Show How Incydr Meets Compliance Needs

When it comes to data loss protection, sometimes it comes down to checking a compliance box. But, according to the Data Exposure Report, 73% of cybersecurity leaders agree that data regulations are too unclear to adhere to, while 68% state they're not fully confident their company is complying with new data protection laws. It's extremely important to show the executive team and board exactly how Incydr meets those compliance needs. Incydr offers complete visibility to your data exposure, as well as effective response controls, such as blocking and security training videos, to control or reduce that exposure.

Resource

- How Incydr Supports Your Compliance And Aligns With Security Frameworks From CIS to NIST

5. Level Up from the Technical Details

Last but not least, resist the urge to get too technical. The executive team and the board cares most about how Incydr helps protect the business (and the bottom line). So, focus on the business results and why Incydr is a must-have security solution to help prevent data loss and the financial and reputational risks that accompany it.

With these tips, you'll be more equipped to gain support from your executive team and the board, so that you won't be one of those stories in the news.

Looking for more leverage? See how current customers drove budget for Incydr **in this infographic.**

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.