netwrix

Top 3 Ways Departing Employees Steal Your Data

www.netwrix.com

Cybercrime keeps evolving, but one thing stays the same: the biggest security threats are often not outside your company, but inside. The problem isn't limited to large organizations; in fact, small and mid-sized businesses fall victim to employee data theft even more often, though these breaches are less likely to make the headlines.

No IT pro wants to be the one to tell the CEO or CIO that an employee has stolen critical data on the way out. The first step in preventing such theft is understanding why and how people are stealing data before or after they depart from their organizations. This article reveals what industry research has discovered about the motives behind this data theft and explores the top three threats that insiders pose to your sensitive data.

What are the motives?

Why do people to take a risk and steal from their employers? According to the 2017 Verizon Data Breach Investigations Report (DBIR), the primary motive is financial gain, which accounted for 60% of breaches in 2016. This is not a surprise. Personally identifiable information (PII) is extremely valuable on the black market, and stolen intellectual property (trade secrets, sales projections, marketing plans and so on) can be worth billions of dollars to competitors. Less frequent motives for data theft are cyber espionage for career development, revenge, whistleblowing and stealing data for fun — but, of course, these motives can also have a strong financial component.

What happens to those who underestimate the risk of employee data theft?

How exactly does data theft play out based on these different motivations? Here are three case studies that illustrate the process, and the consequences for the victim organizations.

CASE #1

Data theft for financial gain and career development

Here's how quickly a dream can turn into a nightmare. Uber is one of the most successful and well-known companies in the world. To advance its goal of developing self-driving cars, it acquired a startup called Otto, which was developing a technology Uber needed, and hired its all-star team, including Otto's founder, Anthony Lewandowski. Uber seems well on its way to dominance in the hot new area of autonomous vehicles.

A year later, Uber's lesser known competitor, Waymo, sued Uber for trade secret theft.

A developer stole 14,000 confidential technical documents, blueprints, and other files and used that intellectual property to found his startup

According to Waymo, Lewandowski stole some 14,000 confidential technical documents, blueprints, design files and other files as he was leaving Waymo and used that intellectual property to found his startup, which was later acquired by Uber. Now Uber is in a very tough position. It may face criminal prosecution not only for using stolen technology in the production of its self-driving vehicles, but also of actively covering up the trade secret theft.

The case is under investigation and the trial has been postponed to December 2017, but both companies are already involved in a series of intense public hearings. This certainly doesn't look good for Uber, especially considering the fact that the company is facing another federal investigation for allegedly violating the U.S. Computing Fraud and Abuse Act (CFAA).

It's too early to predict how the battle between Uber and Waymo will end, but stakes are already high: companies are fighting for the right to develop a technology that may be as significant for the industry as the invention of the automobile itself.

CASE #2

Deliberate data theft or damage

It would be horrifying to discover that photos and videos of your plastic surgery have been posted on the internet — especially if you're a celebrity whose face can be readily identified by millions of viewers. But that's exactly what happened to patients of famous Beverly Hills plastic surgeon Dr. Zain Kadri.

In 2016, Kadri hired an employee who worked first as a driver and translator, and then moved on to data entry and answering phone calls. She either quit or was fired in 2017 after being accused of embezzling from the company.

An employee with privileged rights used her corporate smartphone to take pictures of patients' medical records and credit card information

But apparently she misused her insider privileges in other ways. According to a statement from Kadri's practice, she also used her corporate smartphone to take pictures of patients' medical records and credit card information — and also took inappropriate photographs and videos of patients before and during surgery.

The case is still under investigation; however, Kadri believes that the primary motive here is revenge. At least some of the videos and photos were made public on Snapchat and Instagram — a strategy that **could draw ire towards Dr. Kadri from his celebrity clientele and hurt his practice**. So far, there is no evidence that the employee was financially motivated or hired by a competitor.

CASE #3

Human mistakes or negligence

It would be horrifying to discover that photos and videos of your plastic surgery have been posted on the internet — especially if you're a celebrity whose face can be readily identified by millions of viewers. But that's exactly what happened to patients of famous Beverly Hills plastic surgeon Dr. Zain Kadri.

In 2016, Kadri hired an employee who worked first as a driver and translator, and then moved on to data entry and answering phone calls. She either quit or was fired in 2017 after being accused of embezzling from the company.

In February 2016, an employee at the U.S. Federal Deposit Insurance Corporation (FDIC) was leaving her job. On her last day at work, she downloaded her personal files from her work computer to a USB drive and took it home. Three day later, the FDIC's data protection software detected that 44,000 customer records, including PII, had been accidentally taken along with her personal data. The FDIC promptly contacted the ex-employee and asked her to return the device and sign an affidavit stating she did not use or share the information.

> **The FDIC had already experienced at least 5 security incidents, with departing employees accidentally transferring company data to personal storage devices**

This case wouldn't be so worrisome if the FDIC hadn't already experienced at least five similar security incidents, with departing employees accidentally transferring company data to personal storage devices — including highly sensitive data like loan and banking information. Unlike the February 2016 incident, not all the earlier breaches were immediately handled and reported by FDIC, which led to a series of hearings and fines from regulatory bodies.

Although the FDIC seems to have taken to heart the need to report security incidents promptly, the management team should really ask two key questions: first, how long will it be before the organization finally updates its security policies and makes sure that employees follow basic cybersecurity rules? And second, were all of these breaches truly unintentional?

A ticking bomb: who's next?

All the cases above have one thing in common: it took less time for ex-employees to obtain sensitive data than for organizations to detect and investigate the incident. Indeed, stealing an employer's data doesn't take long — you need only a couple of minutes to copy sensitive files to your personal device. But detecting a malicious insider in your company's network can be challenging; the DBIR found that data theft can take months or years to discover.

The simple fact is, you can't get inside the head of employees and know whether they are planning to resign and whether they plan to take your critical data with them when they go. Therefore, you need to treat every employee as a ticking bomb who can cause a security horror story. Specifically, you must take proactive steps to prevent data theft and have strategies in place to detect cases you can't prevent. Unfortunately, the 2017 Netwrix IT Risks Survey revealed that most of organizations still have only partial visibility into what users are doing in their IT environments — which makes these goals difficult to achieve.

Start Using Netwrix Effective Permissions Reporting Tool

The Netwrix Effective Permissions Reporting Tool helps you make sure that employees' permissions align with their roles in the organization. The freeware tool automatically delivers you a daily report that **helps uncover excessive permissions in AD and file shares** and details how the access was gained.

Start Using Free Tool

Get it free of charge

Never expires, so you can be sure it'll be there for you when you need it most.

Monitor who has access to what

See users' AD group membership and file share permissions in a single report.

Simplify your IT team's life

Track down any user's permissions across both AD and file servers in a few clicks.

Ensure compliance

Proof that all permissions are aligned with HR job descriptions and employee roles.

Corporate Headquarters: 300 Spectrum Center Drive, Suite 200 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749

EMEA: +44 (0) 203-318-02