Veriato

How UEBA

Mitigates IP Theft by Departing Employees

An introduction to the benefits of User and Entity Behavior Analytics in assessing employee behavior

By Derek A. Smith (CISSP)

www.veriato.com

The class of cyber actor with the greatest capacity to cause harm to organizations is not the so-called state-sponsored hacker or cyber-terrorists. It is the "insider" – the company's employees, ex-employees, and trusted vendors. Most IT systems are protected by defensive technologies which present a significant hurdle to unauthenticated outsiders. However, the company insiders have authentication credentials that allow them past the defensive technologies and provide them with access to the company's intellectual property.

CASE STUDY:

Consider George, a senior sales rep. George understands the value of relationships. When he started his current position ten years ago, he brought in his collection of hundreds of business cards and notes, and set to work entering that information into his employer's CRM.

Over the years, George dutifully entered information about his clients that would help him relate to them on a more personal level – including the types of gifts the client preferred during the holidays. Other employees also added supporting details and customer information.

George is now preparing to start working for a new employer as their VP of sales. To help him get off to a great start in the new company, George downloads his current employer's customer database. His rationale is that much of the current data was from his hard work and his personal contribution from his former collection of business cards.

While George may believe that he has a legitimate claim to the customer information because he brought in hundreds of new names and personally worked cultivating those and other relationships for a decade, all the information in the CRM belongs to the employer. George's transfer of his current employer's valuable and confidential digital assets, is theft.

The current employer will likely have an actionable legal claim against both George and his new employer. However, successfully defending that claim will depend on the current employer's ability to provide objective evidence that it was George who downloaded and transferred the digital assets.

Of course, the very nature of digital assets is that they are highly transitory and readily copied. Without a reliable means to objectively provide evidence of misconduct on the part of a departing employee, the employer has little recourse against either the former employee or the former employee's new employer.

CASE STUDY:

Sally, a dedicated application developer, spent much of the last year writing code for a set of highly interchangeable software modules as part of her company's larger project to expand their microservices platform.

Sally coded her modules in such a way that they could be utilized across a broad array of applications. She likened the modules to the tools in a mechanic's toolbox.

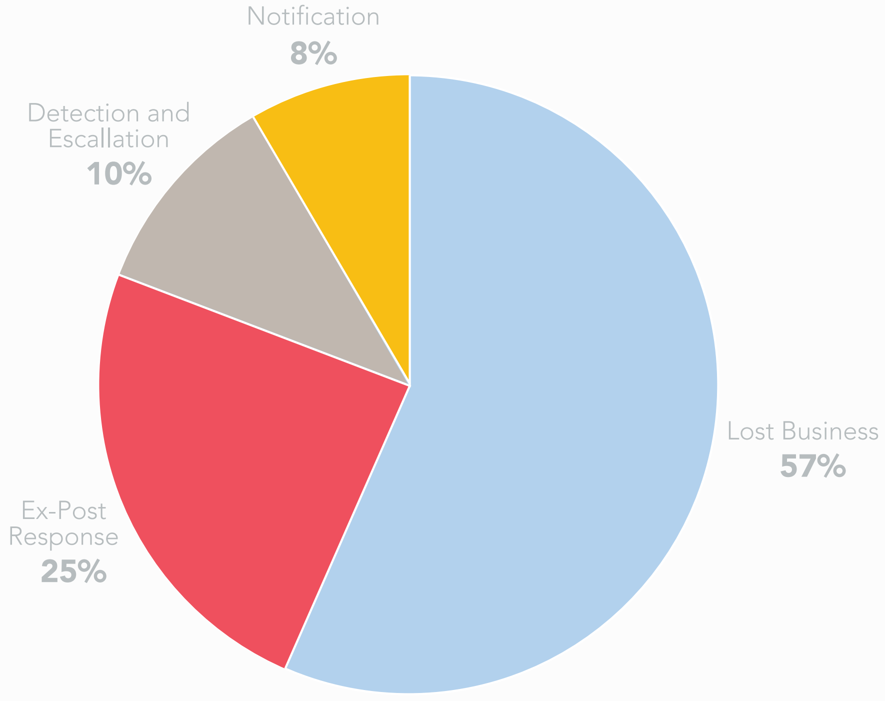
Since developing the modules consumed most of her working time, and even required her to work from home on occasion, she freely kept a copy of the source code on her personal laptop.

Sally is now planning on starting her own IT consultancy – based on her work coding the modules. After all, she reasons, the modules are her baby and no one else really understands the coding or effort that went into creating them.

Unfortunately, Sally is wrong about the ownership of the source code. Because she developed the code while in the employ of another and for her employer's purposes, the source code belongs to the employer, not Sally.

Even though a copy of the source code resides on Sally's personal computer, it still belongs to the employer.

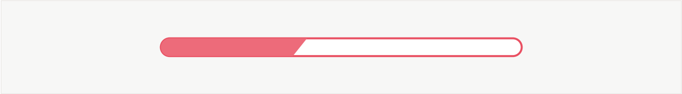
Breakdown of the Average Cost of a US Data Breach



Quantifying IP Theft by Employees

These are just two hypothetical examples of employees stealing intellectual property (IP). A recent security survey demonstrated that 87% of departing employees take data that they worked on during their company tenure, and 28% take data created by others.[i] Data pilfered includes financial, confidential consumer information, price lists, marketing plans, sales data, competitive intelligence, design specifications, and other intellectual property. While data breaches involving confidential consumer information routinely makes the news – and may be costly for companies regarding direct and indirect costs – theft of a company's IP can be devastating. Depending on the nature and amount of IP removed, a company can lose its competitive position, or even be in danger of no longer existing.

According to another recent study, as many as 74% of data breaches originate from insider threats. [ii] To quantify that in terms a CFO or board of directors can appreciate, consider that the average US data breach costs just over $7 million, with a self-reported likelihood of experiencing a breach in a given year of 92%. Thus, of the Fortune 1000 companies, each year approximately 680 of them can expect to experience a financial loss of, on average, $7 million,[iii] due to employee accidents or malicious behavior.



How Employees Steal Intellectual Property

Technology is a double-edged sword. On the one hand, it allows organizations to generate tremendous economic gain through data mining, advanced analytic capabilities, and the nature of a highly-interconnected ecosystem to connect sellers with ideal buyers.
However, that same technology makes it possible for employees to quickly make off with whatever data to which their authentication credentials give them access:

- Thousands of customer names and all their associated information – data that 20 years ago would have consumed reams of paper – now fit on a single thumb drive that easily fits into a pocket.

- Smartphones are readily connectible to company wireless networks. With enormous storage capacity, the now ubiquitous devices can be used to effortlessly exfiltrated many gigabytes of data through the company's front door or from any remote location with a WiFi connection.

- Email and messenger services provide a convenient way for employees to send large volumes of confidential documents to their personal home computer.

- Working remotely allows employees to access the company system from their personal computer.

General Recommendations for Preventing IP Theft

Despite the existence of current laws intended to protect companies from IP theft and company policies and employee training, the prevalence of employee theft of company IP continues. However, there are specific steps companies can take to mitigate the possibility of IP theft or to protect their interests in the case a theft is realized.

- Employees should have the lowest level of credentials which still allows them to be able to complete their job functions. Not only will this prohibit employees from accessing company information that is not necessary for their work, but in most cases it will also prohibit the installation of any hardware or software that can be used for the exfiltration of data (i.e. being able to create CDs or DVDs, or to copy data to a thumb drive).

- Consider configuring of firewalls to block malicious websites or those which can be used to transfer data.

- Encrypt all data at all stages of storage and transport and require user authentication to utilize encrypted data.

- Keep detailed records of employee interaction with the company's digital assets – particularly any action whereby the employee downloads, emails, IMs, or transfers digital assets to removable media.

- Once HR is informed that an employee will be leaving – whether voluntarily or involuntarily – increase monitoring of that employee during the departure period.

- Conduct a detailed exit interview to discuss the employee's duty to return all company property and assets – including all copies of digital assets.

How Veriato's UEBA helps prevent Employee IP Theft

Psychologists and employee managers have long known that a person's behavior can provide subtle insights to their state of mind. Humans can intuitively process these subtle changes to get a "sense" of when a trusted employee is becoming a "rogue insider." However, it would be impractical, if not outright impossible, for an organization's cyber security staff to observe and monitor each employee for the telltale signs indicating in increasing probability of IP theft. Today's computer systems, though, do have the capacity to monitor each user. User and Entity Behavior Analytics (UEBA) – a solution that uses advanced machine learning algorithms which can approximate human insightfulness powered by the Veriato platform – has the ability not only to monitor each user on the system, including automated administrative "users," but to compare each user's real-time activities against their recorded behavior baseline.

Veriato Recon analyzes insider behavior based on the users' psycholinguistics and activity, then compares that behavior to recorded baselines. When anomalous behavior or linguistic shifts that may indicate a shift toward the user becoming an insider threat is detected, an alert is sent to security and HR that more careful monitoring may be warranted. Veriato Recon keeps a rolling 30-day record on each local computer in a fully encrypted file of user activity, providing the most accurate picture of what an employee is doing.

Veriato 360 provides unparalleled monitoring capabilities into employee online use and communications, without getting in the way of legitimate productivity. Data collected can be easily reviewed through rapid reporting, an intuitive dashboard and video playback of activity.

User and Entity Behavior Analytics watches for signs of change that indicates a trusted employee is becoming or has become a “rogue insider threat” and alerts the proper personnel as soon as meaningful variances from the individual’s baseline behaviors and language are detected. Armed with Veriato 360 and Veriato Recon, organizations can proactively respond to potential IP theft from departing employees and protect themselves from the harm that would otherwise occur.

[i] Glenister, Daren. ”Safeguarding Data when Employees Leave the Company.” Cloud Tweaks: New York. February 17, 2017.
https://cloudtweaks.com/2017/02/safeguarding-data-employees-leave-company/

[ii] “Clearswift Insider Threat Index (CITI): US Edition.” Clearswift Corporation: Mount Laurel. 2015.
http://pages.clearswift.com/rs/591-QHZ-135/images/Clearswift_Insider_Threat_Index_2015_US.pdf

[iii] “2016 Cost of Data Breach Study: Global Analysis.” Ponemon Institute: Traverse City. June 2016.
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410
+1 888 598 2788
sales@veriato.com

Veriato EMEA
3rd Floor,Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom
+44 (0) 1483 662888
sales@veriato.com

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/Veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/