THE HR EXIT UPDATED AND SECURED!

MANAGING EX-EMPLOYEE RISK IN THE DIGITAL AGE

CALVIN LIU

Copyright © Calvin Liu, 2018

The author reserves all rights to this publication. Permission is not granted anyone to reproduce or transmit any part of this book through any means or form be it electronic or mechanical. Permission is not granted for the right to store the information herein in a retrieval system, nor is permission granted for the right to photocopy, record copies, scan parts of this document, etc., without the proper written permission of the publisher or author.

Disclaimer

All the information in this book is to be used for informational and educational purposes only. The author will not account in any way for any results that stem from the use of the contents herein. While conscious and creative attempts have been made to ensure that all information provided herein is as accurate and useful as possible, the author is not legally bound to be responsible for any damage caused by the accuracy as well as use/misuse of this information.

Contents

To the love of my life

without whose support,

none of this would be possible.

Foreword

By Maria Zelies

When Calvin informed me that he had written a book about the HR Exit Process, and asked if I would write a foreword – I was skeptical. I was certain that a book on the HR Exit Process would be as outdated as the practice itself. How can any book pack in novel ideas and insights into this concept or help organizations achieve breakthroughs? Many companies have done away even with HR Exit interviews; some have even labeled that practice as "One Worthless Activity HR Has to Handle".

This was my starting point in reading this book.

As I delved further into the first chapters, I expected to see the same routine analysis. Instead, as the title notes, it is a thorough review of the lessons learned on what HR Exit practices work followed by an in-depth exploration of vital issues that are now arising due to the turbocharged use of technology in enterprises all over the world and in every vertical. This book is not

just focused on the novel but explores how technology enables more productivity but also greater harms when used by unscrupulous employees, as examined in the section: "Is There Significant Risk Posed By Departing Employees?"

There are also many first hand anecdotes, shaped by the evidence and experience, to lead the HR leaders and enterprises through a journey through the world of technologies and potential employee misconduct. Calvin explores the future with such topics as: "The HR Exit Process of Tomorrow" His focus is really not on bringing anything new but what enterprises must do to sustain the test of time and technology, concentrating on the topics that are most essential to understanding the HR Exit Process in the digital age.

I was also comfortable with the user-friendly structure and practical content in this book. Liu leaves out the jargon and makes it easy for the reader to digest by dividing his advice.

As a cybersecurity and digital forensics expert, it make sense that Calvin zeros in on the technology. The reader will find none of the over-hyped trivia and nonsense waiting for you in outdated HR 101 business writing and presentations. In the chapter, "Types of Valuable Company Secrets", for example, he digs into the key lessons that matter most, such as how enterprises must recognize the digital nature of their competitiveness and the need to adapt to employee misuse, misconduct and mistakes in today's digital age.

The usefulness of this book comes from the various business case studies presented on leadership, experience and failures at various organizations. The essential piece of this really not about the HR Exit Process as we all know it but really on the lifecycle of the departing employee and the risks, measures and opportunities that enterprises need to be aware of due to changes brought by today's digital age.

I hope you learned as much as I did.

Maria Zelies, J.D., specializes in legal and compliance for a broad range of clients and industries, with significant labor and employment experience. Maria was most recently general counsel at a US registered advisor, and was formerly practicing law at Dewey Ballantine, Weil Gotshal and Credit Suisse. Maria holds a B.A. from UCLA, a J.D. from UC Berkeley School of Law, and a M.Sc. from the London School of Economics.

CHAPTER ONE

HR Today

The HR profession today (2018) focuses heavily on talent acquisition, onboarding, talent management, benefits and so forth – areas associated with starting or ongoing work.

Yet for the corporation that lasts, the reality is that every employee that starts work or is presently working will, at some point, exit. Sometimes this is due to retirement, but lifelong employment in a single institution is vanishingly rare in today. Given the reality of the modern employee life cycle, the HR Exit process is just as important as talent acquisition, onboarding and management.

This book was created to address that portion of the employee life cycle which has been neglected: the HR Exit Process.

The HR Exit Process of Today

The HR Exit process today is primarily that of the HR Exit interview. The HR Exit interview is primarily aimed at informing the employer on the reasons and/or circumstances as to why an employee is voluntarily departing.

Even in cases of termination, the exit interview can provide valuable feedback to improve the employer's organization and processes. In both cases, the impending departure provides the employee the opportunity to express his or her feelings, impressions and concerns about their time with the employer. The employer has the opportunity to learn what they are doing right and to learn about areas that need improvement; issues encountered by the employee during the course of the work can be identified for future resolution. Even for terminated employees, the employer has

the opportunity to learn the cause for the under-performance – some of which may be remedied.

The overall HR Exit process beyond the HR Exit interview is important to ensure that required forms are completed, post-termination rights and responsibilities are communicated and that the employer has executed security and infrastructure updates to reflect the change. Increasingly, platforms like Workday help to automate the IT updates reflecting termination of employment.

Conducting the Exit Interview of Today

Honest feedback, whether positive or negative, is the goal of the HR Exit interview and is why the HR Exit interview should be conducted by a human resource specialist in the company or a skilled third party.

The exit interviewer should be a professional with whom the employee can be comfortable enough to share: what they like, what they don't like, or other observations whatever the case may be. It is an opportune time to get candid reactions which otherwise can be difficult to solicit. These reactions can provide extremely valuable insight into the systems, management, policies and working conditions of the organization.

The HR Exit interview can also be an opportune time to confirm the experience and skill sets

required for the job; to garner useful knowledge, information and contacts from the existing employee; and importantly, a means to depart on the best possible terms. It is essential that the HR Exit interview is a standard procedure forming a company's out-processing flow.

Some companies like to conduct the HR Exit interview using a questionnaire. Use of questionnaires has limitations, however, because they do not provide opportunity for clarification or follow-up questions should the need arise, nor is there the presence of an HR professional to assess the mood, tone and body language of the employee.

For example, if an employee indicates *compensation* as a reason for exiting the organization in a questionnaire, this format does not allow the opportunity to explore what the issue is with his or her compensation. Not all

compensation issues are a function of absolute levels of salary or wages – perhaps it is the lack of a leave program after 7 years of employment or the need for elder care benefits. Perhaps there is insufficient or inaccurate benchmark compensation information being used by the employer.

The experience and flexibility of an open, person to person interview is why many successful organizations opt for the more personal touch of a face-to-face HR Exit interview as part of the overall HR Exit process.

Even face to face exit interviews with experienced and skilled HR professionals can still be improved.

- Due Process: Without follow up to the gathered data, much of the benefit of successful HR Exit interviews is lost. The HR Exit process should include procedures to follow up on feedback in

order to promote ongoing improvement. Furthermore, a failure to follow up can negatively impact the morale of current employees because this failure may be construed as employer indifference to employee input.Mindfulness: Organizations develop their own personalities and culture. The HR Exit interview can provide a way to learn about significant issues which are otherwise not being highlighted due to existing internal dynamics. Catching such issues is always good, but the HR Exit interview is not the ideal point where a company first becomes aware of such problems – as if it takes resignation for the company to hear the employee's opinion.

- Data: Feedback from exit interviews can inform a number of important areas including competitive compensation benchmarking as

well as the effectiveness and style of management.

The modern HR exit interview process also has to take into account the role of IT in the modern workplace.

IT has greatly changed how work is conducted today – both from communications and an overall productivity standpoint. HR Exit processes and checklists should ensure that email access, data access on both on-premise and cloud information systems, 3rd party SaaS tool accounts like SalesForce, building access, company provided equipment like laptops and cell phones and so forth are properly handled. Use of a modern HR platform like Workday can be very beneficial to ensure that the IT infrastructure is updated to reflect the terminated privileges and access formerly given to the departing employee.

The HR Exit process should also validate that outstanding expense reports are filed and processed, vacation or other leave days are accounted for and that accompanying documentation is provided.

A sample HR Exit Process Checklist is provided in the appendices.

Closely related to IT is intellectual property and trade secrets. Company materials on cell phones, computers and cloud storage should be returned or destroyed much as physical brochures, documentation, company memos, books or other materials should be returned.The modern HR Exit process needs to take into account potential employee misbehavior. ModernIT systems such as those mentioned previously, while greatly increasing productivity, also greatly increase the scope of damage which some unscrupulous employees may cause. While non-compete and

non-disclosure agreements are fairly commonplace, the reality is that IP and trade secret theft still occurs. The HR exit process thus also needs to address this risk.

Traditionally, instances of ex-employee misbehavior have been addressed through lawsuits and professional investigations. There have been many such examples in the news:

The Waymo division of Google sued Uber over the copying of thousands of internal Waymo documents by a departing employee. The employee formed a new company which was acquired by Uber the same day of formation. The lawsuit was eventually settled for $245 million in stock based compensation.[1]

An ex-Apple employee was arrested by the FBI for allegedly taking information from Apple's

[1] https://cleantechnica.com/2018/02/10/uber-settles-waymo-google-245-million-stock/

autonomous vehicle division to his new employer – a Chinese company called Xmotors.[2]

In my own work at Ventura Enterprise Risk Management, a cyber security startup that I cofounded in 2015, I have investigated dozens of examples of trade secret and IP theft by former employees ranging from mundane the theft of customer lists to the theft of an entire startup!

The startup was a payment processing enterprise with a non-technical founder who hired a friend to create the technical team. 2 weeks before this startup was to take its product public, the CTO/friend left the company but not before deleting all Google, Slack and AWS cloud data. 1 month later, the ex-CTO formed a new company with a different name but offering the same type of payment processing product. Our investigation

[2] https://techcrunch.com/2018/07/10/ex-apple-employee-charged-with-stealing-self-driving-car-secrets/

subsequently showed the new company's online product still contained mentions of the former employer's company.

From the above examples, departing employee misbehavior is real.

But is this a significant problem, or are these examples just a few bad eggs?

CHAPTER TWO

Departing Employees Represent Risk As Well As Open Reqs

Before examining the risk of malicious employees, some terms defined:

Definitions

Artifact

1) An object made by a human being, typically an item of cultural or historical interest.
2) Something observed in a scientific investigation or experiment that is not naturally present but occurs as a result of the preparative or investigative procedure.
3) In this book, artifacts are cyber forensics data in the form of files, database, cookies, system logs or other data sets which are not normally accessible to the typical user.

Digital Forensics

A branch of forensic science encompassing the recovery and investigation of material found in digital devices.[3] The term was synonymous with computer forensics but the latter term is commonly used anymore because forensics requires investigation for all devices that can store digital data.

Forensic Imaging

Forensic imaging is the process of obtaining an exact bitstream copy of the original strong media that exists on the subject computer. [4] It is also known as a bit for bit, sector for sector copying or forensic acquisition. Beyond obtaining files visible to the operating system, forensic imaging can recover deleted files. In other words, further evidence can be provided

[3] https://en.wikipedia.org/wiki/Digital_forensics
[4] https://www.forensicon.com/resources/articles/what-is-forensic-hard-drive-imaging/

in form of files that have been deleted to prevent discovery in scenarios of trade secret misappropriation and copyright infringement.

It is notable that as much as forensic imaging can detect employee malicious acts, it can also be used to prevent the loss of important and critical files in the first place.

Metadata

Data (information) that provides information about other data.[5] In other words, metadata describes the content of another item – say an image or a text document, even web pages.

The types of metadata include Structural metadata, Administrative metadata, Descriptive metadata and (the recently developed) Accessibility metadata.

[5] https://en.wikipedia.org/wiki/Metadata

PII

PII is an acronym for Personality Identifiable Information[6]; information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Examples include credit card numbers, social security numbers, addresses, phone numbers, logins, passwords, IP addresses, etc.

Shadow IT

This involves information-technology systems and solutions built and used inside organizations without explicit organizational approval.[7]

Examples of such systems include Dropbox, Facebook, Twitter, Instagram, Slack, Teamviewer, etc.

[6] https://en.wikipedia.org/wiki/Personally_identifiable_information
[7] https://en.wikipedia.org/wiki/Shadow_IT

A study confirmed that of every 20 SaaS (Software as a Service) apps, 7 are used unapproved and therefore without oversight; it also showed that the largest percentage of shadow IT users are IT employees, apparently, they feel the risk of usage can be better handled by them.

Shadow Communications

Communication technology systems and solutions built and used inside organizations without explicit organizational approval or support; you can consider this as a subset of Shadow IT. Examples include WhatsApp, Messenger, SMS or text messaging, Skype, WeChat, Lime, Telegram, Slack, private email, etc.

A study showed that 35% of employees feel some protocols need to be sidelined for work efficiency, while 63%, against a proper

judgment, transfer their work home through their private email to continue work from there.

Malicious Insider

A malicious threat to an organization can come from people within the organization such as employees, former employees, contractors or business associates who have inside information concerning the organization's security practices, data and computer systems. These threats may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems (Definition source: Wikipedia on Insider threat).

An insider within an organization is acquainted with the organization's data, intellectual property and schemes put in place to keep them protected. The insider may also have legitimate access to the organization's internal network and computer systems – to serve him or her in

their professional duties; these make it easier and almost undetectable for such an individual to bypass security measures to gain physical access to sensitive files of which they don't even hack into the company's network.

Do Departing Employees Pose Significant Risk?

We have talked about how the HR Exit process of today can provide valuable feedback to improve an organization, to learn about industry benchmarks such as in compensation and to potentially promote a positive ongoing relationship with the departing employee. While the majority of departing employees are indisputably honest and honorable individuals, the statistics show that a visible percentage of employees are neither honorable or honest. There aren't good statistics to tabulate the precise percentage of employees are malicious insiders are, but there are some examples showing that this is almost certainly a severe problem.

Computer Economics published a study showing that more than half of all firms surveyed suffered

at least one malicious insider attack in the previous 2 years.[8] Using the average number of employees from the 2014 NAICS data, the 24% national turnover numbers from the US Bureau of Labor Statistics (BLS, with 9.3% for federal government turnover), and furthermore assuming attacked firms only suffered 1 incident, the minimum possible rate of malicious insider activity due to departing employees may be over 5%.

1 in 20 departing employees may be doing something malicious!

A second data point: The IBM X-Force Threat Intelligence reports shows malicious insider rates from 1% to 25% depending on the sector as compared to all overall cyber attacks:[9]

[8] https://www.computereconomics.com/article.cfm?id=1537
[9] https://www.cyberscoop.com/health-care-industry-king-malicious-insider-threat/

Attack sources by industry

1 January 2016 through 31 December 2016

	Industry sector	% Malicious insider	% Inadvertent actor	% Outsiders
1	Financial services	5%	53%	42%
2	Information and communications	1%	3%	96%
3	Manufacturing	4%	5%	91%
4	Retail	2%	7%	91%
5	Healthcare	25%	46%	29%

Fewer

More

To put these numbers in perspective: a medium sized bank will experience thousands of attacks per week. Cyber security is a $90 billion dollar revenue industry; insider threats are a significant fraction of overall cyber security risk and must be kept under consideration.

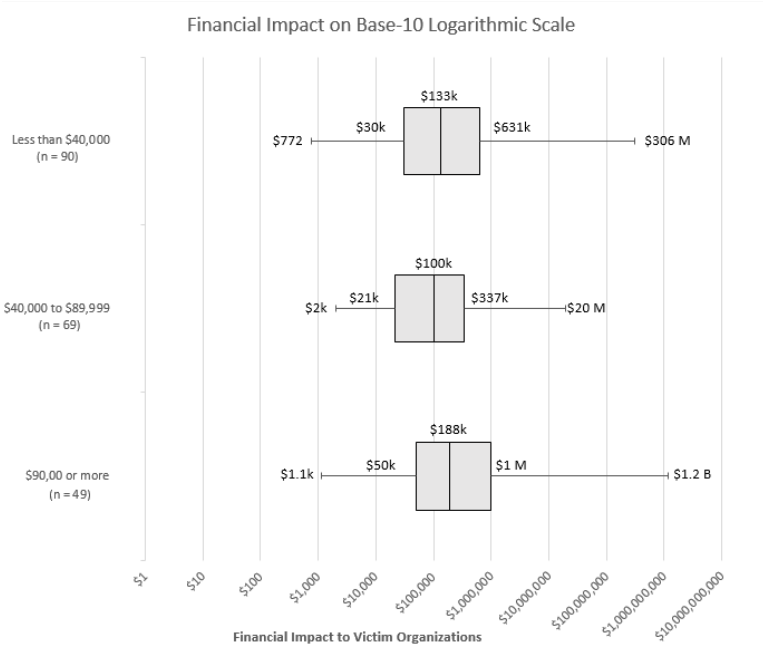
Losses from Malicious Insiders

We've examined some reports of the frequency of malicious insider attack. What about the cost?

A study made at Carnegie Mellon university gives us some insight.[10] The study examined 820 insider incidents reported to the US CERT – which is the US government Cyber Emergency Response Team – and even broke down costs from each incident by salary category.

The average cost per incident is well over $100, 000 irrespective of the salary of the employee, and the largest examples of loss in each category were tens to hundreds to over one billion dollars.

[10] https://insights.sei.cmu.edu/insider-threat/2016/07/how-does-insider-gender-relate-to-type-incident.html



Of course, national average frequency and loss data doesn't itself help an organization understand just how much financial risk is represented by malicious insider activity. To help interested professionals assess their potential level of malicious departing employee risk, a FAIR (Factor Analysis of Information Risk) model is included in the appendices.

Who Should Be Worried?

Apple, Tesla, Google, Genentech and Micron are all tech companies that have suffered from public examples of departing employee misbehavior just in 2017 and 2018.

Do other companies have to worry as well?

While many companies do not have explicit intellectual properties like tech companies, the reality is the every company has some kind of information worth protecting. It is an unusual company that doesn't have something that separates it from existing and potential competitors, and we will examine the major categories at risk from malicious insiders and ex-employees.

Most importantly, consider how much greater access and capability exists to steal trade secrets, customer lists, intellectual property or other types

of information vital to an organization. 25 years ago, the standard floppy disk could contain about 1000 pages of documents or 2 modern era digital photos. A CD could contain about 500 times more than a floppy disk – call it 500,000 pages of documents or 1000 modern photos.

A modern USB external hard drive holds 12 times more data than a CD, can copy data hundreds of times faster. A shadow IT cloud storage app like Dropbox can upload the entire contents of the aforementioned USB external drive in a week.

Moreover, data access today is much easier. In the past, attackers would have to access scarce and restricted central server systems, often physically and for long periods of time, in order to copy data. Today, networks allows remote access to anyone with the appropriate credentials. As Edward Snowden showed – this type of access can yield

tremendous amounts of data as the Snowden archive is reportedly 1.7 million documents[11].

[11] http://www.bloomberg.com/news/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.html via https://archive.is/cEy9j

CHAPTER THREE

Types of Valuable Company Secrets

1) Company Operational Information

A company's operational information assists it in exercising its functions in decision-making regarding and affecting the members of the organization. Examples of such information include rules, regulations, guidelines, precedents, and practices.

The key asset in most organizations is information. Competitive advantage is gained if vital information privy to only key personnel in the company is stolen. Because business opportunities are limited, business

competitiveness is interfered with when there is a threat to acquire or leak this information.

Competitors can learn how the company's processes are superior and where. They can learn who key employees are. Potential acquirers can learn about how profitable or desperate an acquisition target is. Cyber criminals can identify key executives to target phishing or whaling attacks to steal money. Vendors can use internal information to change pricing during sales negotiations.

There are many other cases where internal information can cause significant harm when revealed to the wrong people. One of the most common attacks is to trick companies to wire transfer funds to the wrong location. This type of attack is called BEC: Business Email Compromise.The most typical form is where a company's email is hacked into, then an email

from a CEO or CFO is sent to the payments department to forward funds to the attacker's bank account under the guise of an urgent secret acquisition or some other important and fast moving business deal. The FBI reports that BEC attacks have netted $12 billion dollars in losses from October 2013 to May 2018.[12]

2) Confidential Company Information

The unauthorized disclosure of data and information which relates to the processes, operations, trade secrets, profits, etc. of any organization of which may affect the company's ability to accomplish its business objectives and cause substantial harm to the competitiveness of the company is a breach of confidentiality. Malicious insiders steal or misuse such

[12] https://securityaffairs.co/wordpress/74449/cyber-crime/fbi-bec-eac-losses.html

confidential information to either directly financially benefit or for personal purposes.

An example of this: A UBS banker was accused of leaking identities of clients to other parties for personal gain.[13]

3) Employee PII

Employee PII is particularly useful for criminals or headhunting competitors. Cyber criminals have reaped billions of dollars from stolen employee W2 data – the data is used to file a false return with tax refunds going to the criminals' bank accounts. Competitors in turn benefit greatly from know who key employees are, what they make, how to contact them and even what their HR assessment files contain (i.e. their state of contentment within their present organization).

[13] https://www.wsj.com/articles/how-a-bankers-message-to-a-client-spelled-trouble-for-ubs-1535449109

A real case: An HR professional at Seagate, a California based Electronics Company, mailed a file containing well over 10, 000 employees' W-2s to the contact information given to her.[14]

Another example is the confirmed breach of the PII of 250, 000 Department of Homeland Security employees, and individuals and witnesses involved in criminal investigations.[15]

Employee PII data loss whether from cyber criminal or malicious insider actions cause companies to incur fines, damage from negative publicity and litigation expenses.

[14] https://www.zdnet.com/article/seagate-sued-by-angry-staff-following-phishing-data-breach/
[15] https://www.cnet.com/news/homeland-security-breach-exposes-data-on-240000-employees/

4) False Claims and Employee Lawsuits

False claims are so identified when an employee intentionally makes a case of a fraudulent claim (for payment); when an employee makes or uses a false statement to evade an obligated duty; when an employee intentionally violates the False Claims Act, either by himself or in conspiracy with others.

Examples include fraudulent healthcare billing (healthcare and medical industries are the victims of most false claims, but worker's compensation is another common area of abuse), false billings (e.g. for products and services untendered, falsifying records like forging, alteration of information, etc.), false cost reports, etc.

Employee lawsuits are commonplace. Malicious suits include litigation over unpaid overtime, personal injury, harassment, wrongful termination, discrimination, etc. Countries like Brazil with very strong worker rights laws experience very high rates of employee lawsuits: Brazil saw 3.9 million such cases filed in 2016 with a total employer to employee payments of over $5.3 billion dollars.[16] There are so many such cases in Brazil that Brazil instituted an entire parallel judicial system to handle the workload.

5) Theft and Embezzlement

Embezzlement, also known as employee theft, occurs with the wrongful appropriation of funds that are in the care of an employee in an organization. Embezzlement is one type of

[16] http://epocanegocios.globo.com/Brasil/noticia/2016/12/epoca-negocios-em-2016-brasil-ganha-3-milhoes-de-acoes-trabalhistas.html

white collar crime called fraud; *fraud* is defined as purposeful misrepresentation and/or concealment of information in order to induce a self-incriminating act by – or an act at the detriment of – another, either the employer or another employee. Some types of fraud schemes include data theft, bribery and corruption, accounting misrepresentation, false or inaccurate payroll, asset misappropriation, etc.

Examples of fraud, theft and embezzlement: David Smith, a former diagnostics manager of Quest, incurred $1.2 million in false expenses.[17]

Another example: Suraj Samaroo, an IKEA employee, stole almost $400, 000 in one year by issuing himself refunds for purchased orders

[17] http://www.hrmorning.com/you-wont-believe-these-cases-of-employee-fraud/

made by customers, having mastered the company's phone and mail-order system.[18]

More mundane cases involve employees making off with company properties such as laptops. One example: Coca Cola reported the theft of over 50 laptops by an employee over 6 years, which resulted in the compromise of 74,000 Coca Cola employee information.[19]

6) Trade Secrets

Trade secret, according to the definition of Uniform Trade Secrets Act (UTSA), is "information that derives independent economic value from not being generally known and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." This information includes a wide range from a company's business and

[18] Ibid
[19] https://www.cimcor.com/blog/Coca-Cola-Laptop-Theft-Revealed-January-2014

financial information to its core technology to negative information. For some organizations, examples of trade secrets may be special manufacturing processes; for others, it may be product formula, software code, algorithms, customer lists or marketing strategies. Malicious insiders may steal these trade secrets for financial gain, or even personal social causes.

An example is an employee of a U.S exchange company, who stole more than 10, 000 files containing source code; the value of these trade secrets was estimated to be between $50 and $100 million. The employee confessed to having conspired with two other colleagues to develop their company by using the stolen source code.

7) Intellectual Property (IP)

We have previously mentioned Malware – cybercriminals use malware to steal intellectual property. It has been estimated that IP theft costs American businesses hundreds of billions yearly. Note that IP is the blood that runs in the veins of many enterprises; it is the life behind growth, differentiation, and innovation. Theft of IP, therefore, often leads to loss of revenue, it damages company-customer relationships, and it results in devaluation of the company's brand and reputation.

Products that are birthed from IP theft are marketed faster and cheaper by organizations than if they designed the products on their own. As a result, the company that had invested in the innovation, design, and creation of the product find themselves competing with their own products and worse, at half the price.

Several examples:

1) Several employees of Genentech were accused of providing confidential information concerning new Genentech pharmaceuticals to a "close follower" generic pharmaceutical manufacturer.[20] The appearance of generic alternatives to Genentech (or other pharmaceutical company) products inevitably reduces pricing and thus profits.
2) Several employees of Micron are accused of stealing Micron technology so that a competitor could produce similar products.[21] This is another case of competition arising from the creation of cheaper alternatives using stolen technical data

[20] https://m.sfgate.com/news/article/Genentech-workers-trade-secrets-Xanthe-Lam-allen-13346650.php
[21] https://www.theregister.co.uk/2018/11/01/doj_micron_dram/

3) In 2006; a Coca Cola employee who worked as an executive admin in Atlanta, Georgia attempted to steal Coca Cola secrets, including formulas, to sell to Pepsi.[22]

[22] http://www.washingtonpost.com/wp-dyn/content/article/2006/07/05/AR2006070501717.html

CHAPTER FOUR

The HR Exit Process of Tomorrow

The HR Exit process of today is primarily focused on two areas: getting feedback on the company processes with an eye towards identifying potential improvement and ensuring that the departing employee leaves on good terms with an understanding of their rights and obligations.

The HR Exit Process of tomorrow adds the requirement to mitigate potential malicious employee risk, including theft of IP, trade secrets and confidential company information as well as protection against potential employee lawsuits and actual criminal wrongdoing. Previously, we have covered in depth many of the ways by which malicious employees can cause harm to the

companies they are leaving, the potential rate that it occurs and the high cost for incidents.

In light of this, the HR Exit Process of tomorrow needs to address these risks. The parameters to address this risk are as follows:

- **Cost**

Annual turnover In the United States is over 20%; this means for a 1000-person company, at least 200 employees will depart every year. The US Bureau of Labor Statistics showed that the national average monthly turnover averaged 3.3% in 2017; this number includes both voluntary and involuntary departures. The cost of administering the HR Exit Process of tomorrow must take this into account as it can be significant.

- **Proactive vs. Reactive measures**

Proactive Measures

Proactive measures are intended to prevent harm from occurring. These include:

a) **Cybersecurity:** This deals with handling intellectual property or any other identified, vulnerable assets via active oversight. This includes active monitoring and/or prevention of data copying and technology capabilities like Data Loss Prevention software.

b) **Investigation:** Refers to conducting preliminary investigations on some or all departing employees to uncover active or potential risk via MMO (Means, Motive, and Opportunity), behavioral or other forms of active review. This is a thorough but expensive method; the service of outside forensics professionals conducting

investigations will cost a minimum of $2000 per investigation with an average cost of $10, 000. More complex or wider-ranging cases will run into hundreds of thousands of dollars or more.

c) **Education:** A crucial proactive measure is ensuring employees understand clearly what confidential company information is, as well as what they are and are not entitled to do with confidential company information.

d) **Follow-up:** Once an employee leaves, this does not mean the employee is now completely irrelevant to the company. Besides actively malicious actions like IP or other data theft, the employee might start disparaging the company on social media. Another common occurrence is where the employee refuses, neglects to reveal, or misdirects that they will be employed at a competitor

organization. While this is not automatical evidence of malicious action, it is certainly a commonprerequisite. A follow-up on employees for six months or a year to observe what they say regarding the company and where they are next employed is a proactive measure to be considered vs. the impact of discovering harmful activity through other means.

e) **Legal:** Having employees sign non-disclosure and non-compete agreements.

f) **IT:** Preserving employee endpoints. A major cause of high investigation and/or litigation costs is the failure to perform a forensic acquisition on a departing employee's computer. Professional forensics investigators are able to unlock immense amounts of behaviors, communications, and raw data from a computer.

a. Behavior includes activities like file copying either to external media or cloud storage, as well as not relevant areas looked into – for example, an HR agent looking through research group's files is likely suspicious.

b. Communications encompass not just company email, but third-party applications like private email, WhatsApp, Skype, WeChat or Slack. Knowing who is communicated to and what is communicated is a great resource for investigation.

c. Raw data encompasses the files which the employee has accessed. Leaked data for which copies exist on an employee's computer, for example, places such an employee as a potential source for the leak. Having an admissible chain of

custody forensic images of computers used by malicious ex-employees reduces the investigation and litigation costs dramatically.

d. Social media: While most organizations have policies against personal use of corporate computers and networks, the reality is that this still occurs. The identities of an employee's social media profiles can be extracted from the corporate IT and used for post-departure social media followup.

In general, proactive measures like cyber security or active investigation are very expensive; education is less expensive but not effective against hostile or criminally motivated employees.

A new area for proactive measures against departing employee misbehavior is deterrence through digital evidence and access to digital activity.

While most organizations have compliance policies stipulating appropriate, ethical and legal use of corporate computers and networks, these policies in reality are toothless because few organizations have the demonstrated capability to access, much less monitor such activity.

The field of digital forensics, however, has had this type of access for decades. All computers will store the behavior, communications, social media, browser activity, hardware activity, and much more of its user even without any form of prior setup or special software.

The combination of a legally admissible, forensically sound and complete copy of a

departing employee's computer creates a litigation usable, permanent record of that employee's activity on said machine – a digital footprint of all of their activity. Should this activity be malicious, access to this forensic image reduces investigation cost and promotes better legal outcomes.

More importantly, the demonstrated ability to access such activity will close the otherwise open compliance loop around acceptable computer use policies. Such demonstrated capability to access an employee's digital behavior and activity with legally admissible evidence must serve to deter at least some of the potential offenders. While cyber criminals steal billions every year, the vast majority are white collar criminals – which is to say, they have a very low tolerance of risk.

A significant increase to risk is unacceptable to most, and so the use of digital forensic capabilities

with revamped compliance policies has great potential to affect positive change in behavior.

Reactive Measures

Reactive measures are intended to reduce losses when harm occurs. These include:

a) **Legal:** If employees have signed non-disclosure agreements, confidentiality agreements, and so forth, this can reduce the cost of civil litigation in many cases. However, litigation costs can be further reduced through having admissible, incontrovertible evidence of misconduct reinforcing the presence of legal obligations. Litigation is always a significant cost and risk.

b) **Investigation:** Perhaps a departed employee has turned up at a key position in a competitor. Or information restricted to a small group, including the departed

employee, has been detected outside of the organization. In such cases, active investigation may be utilized. However, if the proactive measure of endpoint capture has not been performed, expensive investigations will become even more so. Active investigations without endpoint evidence will often cost 10x or more what they might cost with endpoint evidence. Use of IT personnel to perform some of these investigation functions is a double edged sword. On the one hand, IT personnel have better familiarity with the logs, artifacts and other endpoint functionality which is used by forensic professionals to conduct digital investigations. On the other hand, an untrained (in forensics) IT staff will often damage evidence or render it inadmissible in court. This is a very adverse outcome because

the cost of investigation and prosecution may be reduced, but the outcomes are often substantially or completely impaired.

CHAPTER FIVE

Balancing Privacy With Corporate Risk Management

One concern with increased access to employee digital behavior are new government policies around privacy rights such as GDPR (Global Data Privacy Rights) in Europe and CCPA (California Consumer Privacy Act).

These laws extend new privacy rights to consumers and, potentially, employees, commonly including the right to delete stored data, to object to inaccurate data, to prevent automated processing, to be able to move data from one system to another, and more.

However, while the case law around such privacy acts is still new, there is a clear precedent for

counterbalancing employee rights vs. potential misbehavior.

Article 6 under GDPR, for example, permits use of and access to employee digital information for the purposes of protecting corporate interests and preventing criminal behavior.

Thus while regulatory privacy concerns do need to be kept in mind, at the same time there is a clear recognition that a balance exists between personal privacy rights for employees vs corporate security and risk management.

Conclusion

Times have changed. The HR Exit process must adapt to the changed reality of employee capability today and the fundamentally information driven nature of modern business competitiveness.

Even just 10 years ago, the standard mode of electronic information transfer was the floppy disk.

Today, a single flash memory device can hold literally hundreds of thousands of pages of documentation. Dropbox and other "shadow IT" cloud storage apps can copy even more through the internet.

Where in the past, communications were primarily via voice telephone calls and email, today employees use a wide range of communication channels ranging from Slack to social media like

Facebook, Instagram and Twitter; to messaging and VoIP apps like Messenger, Whatsapp and Skype; to internet forums.

The standalone PC of decades past is now an interconnected node in a worldwide web of communications and data as well as a portal into all of an organization's secrets via its IT infrastructure.

Employees are more productive than ever, but also have more access to damaging information and ever greater ability to gather and transport huge amounts of it.

The HR Exit process must adapt to handle this change in reality. While the existing HR Exit process goal of employee feedback is still important and worthy, the responsibility of mitigating potential departing employee misbehavior is a greater responsibility.

Nor is this responsibility limited to organizations with formally protected intellectual property like patents or trademarks. In our hyper-competitive world, the processes and practices which mark successful businesses are as much a competitive advantage as the physical processes themselves. Whether it is a customer list held by a sales person, a compendium of suppliers for key inputs for a product, a list of high performing employees, or even the details of negotiations with business partners and customers, every organization has enormous amounts of information which comprise a significant part of its competitiveness.

In light of this, the author's recommendation is to execute proactive measures of education, follow-up, legal agreements and IT Endpoint preservation. These are low-cost insurance and risk reduction schemes to address malicious employee risk whether information theft, fraud or

lawsuits. As a digital forensics professional, the author believes that deterrence based upon the capabilities of digital forensics and closing the acceptable computer and network use policies holds enormous potential for positive change.

Companies with very negative consequences for information theft should, in turn, consider the much more expensive proactive measures like investigation and cybersecurity.

APPENDIX I

FAIR overview

Factor Analysis of Information Risk (FAIR) is a standard quantitative model for information and operational risk that helps information risk, cybersecurity and business executives' measure, manage and communicate on information risk in financial terms (Definition source: www.fairinstitue.org) According to FairInstitute, FAIR "has emerged as the standard Value at Risk (VaR) framework for cybersecurity and operational risk."

In other words, FAIR is a risk management scheme; it deals with information risk analyses and provides a framework for understanding, measuring and performing the analyses of these risks no matter the data size or complexity. The framework it provides is used for strengthening

(rather than replacing) risk analyses processes like risk management or IT risk in an IT environment, often specific to information security management systems.

Indeed, risk cannot be measured in units but it can be measured to a consistent and understandable degree, and used to minimize an organization's risk uncertainty; what FAIR does is to "create an extremely powerful methodology for risk communications and management, where setting up a framework for *risk* management becomes an invaluable tool to present risk ideas." In FAIRness, it renders a wholesome approach to enterprise risk; comprehends the impact time and money will have on your security profile; by using an advanced risk model, risk decisions are challenged and defended; studies and applies risk to every company's assets; your risk management framework enjoys the addition of financial

dimension and of course, it *speaks* in a language anyone can understand.

For too long, information security and operational risk has been fairly managed without enough science and FAIR fills this gap with an immense power that enables the company's risk practitioner to make the best decisions based on meaningful FAIR-provided measurements. While this seeming a lot helpful, it is an engaging and challenging endeavor in practicality; but it is better done than be sorry. TRUTH to POWER: Information Governance Research Community stated the basic FAIR risk analyses which consist of four stages and ten steps:

- Identify scenario components
    1. Identify the asset at risk
    2. Identify the threat community under consideration

- Evaluate Loss Event Frequency (LEF)

3. Estimate the probable Threat Event Frequency (TEF)

4. Estimate the Threat Capability (TCap)

5. Estimate Control Strength (CS)

6. Derive Vulnerability (Vuln)

7. Derive Loss Event Frequency (LEF)

- Evaluate Probable Loss Magnitude (PLM)

8. Estimate worst-case loss

9. Estimate probable loss

- Derive and articulate Risk

10. Derive and articulate Risk

Excel FAIR model

A sample model can be accessed at: www.GRCAgent.com/Insider-FAIR and is freely provided for reader use.

Usage of this model will require the purchase of a RiskAMP license for Excel at : www.riskamp.com.

Use of this model for commercial gain by the use of FAIR requires a license.

Appendix II

Sample HR Exit Checklist

For completion by the departing employee,

in conjunction with their manager

NAME: _____

STAFF ID NO_____

ORGANISATIONAL UNIT: _____

POSITION: _____ **DEPARTURE DATE:** _____

NOTIFICATIONS	**Completed**	**N/A**
HR		
Advise HR of forwarding details (for further correspondence)	☐	☐
Ensure that any accumulated flextime credit or debit is eliminated prior to last day (notify HR if this cannot be achieved)	☐	☐
Finalise outstanding leave applications	☐	☐
Complete Exit Interview	☐	☐
Advise staff/HR if occupied specialist safety roles	☐	☐
Other		
Advise all relevant/affected staff and external contacts of departure	☐	☐
Undertake other local requirements (please specify):	☐	☐

(blank page for checklist formatting)

ITEMS FOR RETURN	**Returned**	**N/A**
	☐	☐
Facilities Management		
Employee ID Card returned/electronic access card	☐	☐
IT		
IT hardware returned - laptops, computers, projectors etc (circle applicable items)	☐	☐
IT software and manuals returned	☐	☐
Pagers / Mobile Phone/ Camera returned (circle applicable items)	☐	☐
Remove company documents from personal computer	☐	☐
Finance		
Purchasing Card and related receipts returned	☐	☐
Credit Card and related receipts returned	☐	☐
Fuel Charge Card and related receipts returned	☐	☐
Motor Vehicle, vehicle keys and travel diary returned	☐	☐
Cab charge card/vouchers returned	☐	☐
Other		
Company files, manuals, books, papers, documents, business cards and other materials returned (hard copy and electronic)	☐	☐
Safety equipment (e.g. safety loan equipment, radiation dose badges)	☐	☐

Employee's Name: Signature:
Date:

Supervisor's Name: Signature:
Date:

Appendix III

Acceptable Use Summary Outline

For A Closed Loop Compliance Policy

I. Scope
II. Roles and Responsibilities
III. Information Security Unit
IV. Management and Supervision
V. Employee's Responsibility for Company Resources
VI. Employee Internet and Email Conditions of Use
VII. Employee Email Privacy
VIII. Employee Personal Accounts – Email and Social Media
IX. Clear Desk and Clear Screen Policy
X. Remote/Off-Site Work
XI. Authorized Software and Viruses/Malware
XII. Employee Telephone Equipment Conditions of Use
XIII. Return of Company Property Upon Termination of Contract
XIV. Employee Privacy Expectations
XV. Disciplinary Action
XVI. Compliance Acknowledgement and Signature

*** NOT FOR COMMERCIAL USE – NOT FOR REPRODUCTION ***

About The Author

Calvin is an electrical engineer by training, attending Caltech in 1987.

He spent 10 years in semiconductors and computer design ranging from Advanced Micro Devices through to a divisional county manager for Synopsys in Japan.

He has been working in the startup space since 2006, culminating in the founding of Ventura Enterprise Risk Management in 2015 and GRC Agent in 2018.

At Ventura, he was part of the team that assisted law enforcement in arresting over 330 cyber criminals, provided incident response to dozens of companies ranging from enterprise to individual consultants and provided cyber expertise to hundreds of millions of dollars in civil litigation.