The Quantified Value of CISSP and CISA Certified Employees

A Strategic Approach to Cybersecurity Hiring and Risk Reduction

Part I

Rick Lucas
Global Recruiters
rlucas@grngrandrapids.com

Thomas Lee, PhD
VivoSecurity
ThomasL@VivoSecurity.com

Abstract

Have you ever wondered what effect **CISSP** and **CISA** certified employees have on the probability of a data breach? Recent analysis has found that the probability for a large data breach can be driven to near-zero by investing in sufficient numbers of **CISSP** and **CISA** certified employees. The **CISSP** and **CISA** certifications can be viewed as the technical and human sides of cybersecurity, and both certifications are equally important.

We propose investing in equal numbers of employees with both certifications as a more cost effective approach for improving security. We recommend best-practice reporting structures that foster independence for **CISA** certified employees.

Article

This article provides a new perspective on how staffing can affect the probability for a PII data breach and shape the culture of the organization. It includes objective information on how to actually reduce the probability of a large data breach.

Recently, statistics based regression models have become available that accurately forecast data breach based simply upon the number of employees with certain certifications within a company. These models are about twenty-times more accurate than current scoring methodologies that are based upon controls, suggesting that adequate staffing is an overlooked, but an important component in cybersecurity. Most importantly, these models show that companies with robust employee-sets of certain certifications have a substantially lower probability for a large PII data breach. These models and how they can be used, are discussed in more detail at the end of this article.

Regression analysis of companies that **did** and **did not** experience data breach, found that the number of employees with just two certifications, was very predictive: **CISSP** and **CISA**. A deficit in the number of employees with these two certifications is an effective predictor of data breach. While there is a diminishing return for hiring these employees to reduce probability for small data breaches, there is no diminishing

return reducing probability for large data breaches. This is important, since it means it is possible to drive probability for a large data breach to near zero by employing a sufficient number of experienced, trained and certified personnel.

The most surprising result from our regression analysis is that employees with **CISSP** and **CISA** certifications are equally effective at reducing probability for data breach. This is a surprise since these two certifications characterize two different aspects of cybersecurity: the technical aspect (**CISSP**) and the human side (**CISA**)—and most of the focus in cybersecurity is on the technical side.

The equal value of **CISSP** and **CISA** certified employees in reducing probability of data breach, suggests a more cost effective way to improve cybersecurity—hire more **CISA** certified employees. **CISA** is not considered a technical certification, and the salary of an employee with a **CISA** certification can, on average, be $50K less than an employee with a **CISSP** certification. Unfortunately, our regression analysis does not tell us the optimum employee ratio for these two certifications, but we can make a recommendation below, based upon what we find among companies with the strongest cybersecurity postures.

Let us begin by examining the **CISA** and the **CISSP** certifications to understand what these certifications mean and why they might be so valuable in predicting data breach. We will also suggest reporting structures for **CISA** and explain how these valuable employees can best be used within an organization.

CISA Certification

CISA (Certified Information Systems Auditor) is a certification issued by ISACA (Information Systems Audit and Control Association). It is the most ubiquitous audit certification, it is globally recognized and requires five years of working experience. This certification is focused on the human side of cybersecurity—complying with good policies and procedures. Employees with this certification often reside in various departments throughout the company.

Perhaps it should not be surprising that the number of **CISA** certified employees, independent of the department they work in, are just as predictive for data breach. For example, we all understand that companies can stop successful phishing attacks, if employees simply do as they are told and don't click a link in their email.

But **CISA** certified employees go beyond cybersecurity. They validate that employees and business processes are not only secure but in line with technical needs, such as a sufficient number of security tokens. Business processes range from HR onboarding, all the way to IT and business policies as well as how finance is interacting with external vendors. They will even validate that technical employees are complying with policies and procedures. **CISA** certified employees can also help identify gaps that cannot be protected with technology.

CISA certified employees audit against policies and procedures most often generated by IT, HR and the cybersecurity group. These groups can also have a **CISA** certified employee, but best practice is to minimize conflicts of interest and for a group not to audit itself. This is because there is often a desire to simply correct a problem when it is found, and not document the issue. While correcting the issue is important, documenting the issue is an important first step in preventing future incidents. It is important to remember

that misconfiguration in IT and failure to follow procedures is a common cause of data breach. For a **CISA** certified employee auditing IT, best practice is for these employees to report independently to the CFO or COO, since IT often reports to the CFO in smaller companies, or the COO in larger companies.

There is value in spreading **CISA** certified employees throughout the company since it also spreads the knowledge. Also, since many departments such as Finance, Operations, and Procurement interact with external systems, organizations, and vendors, it becomes increasingly more critical to ensure proper audits are in place throughout an organization.

Finally, it is important to have **CISA** certified employees in line with the vision of the CISO. To ensure this, it is recommended that they report into the office of the CISO. But since these employees will be working with various department heads, their cost might be allocated back to the department they audit and support.

CISSP Certification

CISSP (Certified Information Systems Security Professional) is a cybersecurity technical certification issued by the International Information System Security Certification Consortium (ISC)². This is most ubiquitous technical cybersecurity certifications, it is globally recognized and it requires five years of working experience. Some people regard this certification to be hard to obtain and perhaps the cybersecurity equivalent of the well-respected Cisco Certified Internetwork Expert (CCIE), although the CISSP is broader and less deep, and the pass/fail ratio is extremely low for the CCIE while the CISSP is challenging, but much easier to obtain. In the UK and across Europe the **CISSP** certification has been granted a qualification level equal to that of a master's degree.

CISSP certified employees are technical. They may be responsible for the systems and infrastructure. Maybe he/she manages the network team or the data center and they can be responsible for securing the remote workforce or securely integrating cloud environments (e.g. SaaS, IaaS and PaaS). There is a **CISM** certification (Certified Information Security Manager, issued by ISACA), which is the manager of these IT groups, but a **CISSP** can be either technical or a manager and that's what generally drives the higher salaries for these employees.

It should not be a surprise that an insufficient number of these **CISSP** certified employees is very predictive of data breach since these employees are tasked with ongoing internal risk assessment, incident investigation, recommending security mitigations both technical and through policies and procedures, and sometimes deploying, configuring and monitoring security controls.

Hiring Ratios

Most larger companies have half the number of **CISA** certified employees compared with **CISSP** certified employees. But there are companies that have the same number of **CISA** as **CISSP** certified employees, and many of these companies stand out as having strong cybersecurity. Example companies are: *The Depository Trust & Clearing Corporation* (DTCC) which is a company critical for clearing trading transactions for the banking industry, the *Nasdaq*, and many banks such as *Citibank* and *Wells Fargo*. It is

hard for large companies like *Citibank* and *Wells Fargo* to avoid small data breaches, but for their size, these companies have good security.

We therefore recommend hiring the same number of audit and compliance employees, as technical cybersecurity employees. We feel that a company can achieve better security with the same cybersecurity budget, since **CISA** certified employees are significantly lower cost than **CISSP** certified employees, and because regression analysis finds the same predictive value for both certifications in forecasting data breach.

Other Certifications

The **CISSP** and **CISA** certifications were not the only certifications found to be important. We found **CISSP** and **CISA** certifications to be most predictive, partly because these two are most ubiquitous and allowed regression modeling of both small and large companies.

There are many other very good and complementary certifications relating to cybersecurity. For example **CISM** was also found to be important, but was not common enough to use in our regression analysis of small companies. Also, including the number of **CISM** certified employees in our regression analysis did not improve the predictive accuracy of our model, suggesting that companies that hire **CISSP** certified employees also hire **CISM** certified employees. We defer to cybersecurity professionals to decide the best mix of complementary training certifications that are right for their enterprise.

Conclusion

Regression analysis suggests that hiring enough trained and certified cybersecurity professionals greatly reduces the probability of data breach—especially large data breaches.

We feel that senior management and regulators should also view cybersecurity from the perspective of the number of trained and certified professionals, rather than micromanage compliance with a set of standard controls. These trained employees will discover risks in an ongoing manner, recommend the right controls as technology, threats and business evolve, and they will write policies and procedures that are right for the business. Regression analysis suggests that ensuring employees are compliant with these policies and procedures is just as important as technical cybersecurity controls.

The Predictive Model

VivoSecurity provides a statistical model that forecasts PII data breach for companies in all industries and all company sizes. The model accurately measures 1st, 3rd and 4th party risk, including cloud risk and risk from contractors—from a non-technical perspective.

The model includes: 1) gathering of predictive headcount information without the assistance of the company being assessed, 2) a history of publicly reported data breaches, and 3) probabilities for data breach as a function of data breach size.

A probability based regression model has many new uses:

Aggregate Risk. Aggregate risk is the risk from the sheer number of vendors and 3rd and 4th party partners. This includes aggregate risk from the cloud: SaaS, IaaS and PaaS. Aggregate risk cannot be calculated based upon cyber-maturity scores and ratings, but it can be calculated by summing probabilities for the individual vendors. Because it is probability based, the predictive breach model is more than twenty times more accurate than traditional vendor rating services.

Vendor Triage. Because of high accuracy, the model often finds just a few vendors most likely to have a data breach. These vendors usually represent most (e.g. 80%) of the 3rd party risk. Triage allows estimating the value of mitigation, then focusing efforts on just a few 3rd party partners. This saves money while also quantitatively reducing cybersecurity risk.

Risk Appetite. Our models allow senior management to set a realistic risk appetite for their company - one based upon data breach frequency as a function of data breach size. Further, it allows executives to weigh the cost of mitigation, the cost of risk transfer and other business priorities.

For further information about the regression model, contact: Hayden McKaskle at Hayden@vivosecurity.com or Inquiries@vivosecurity.com

Model Development & Accuracy

A regression model is a statistical analysis of historical data that identifies factors that can be used to predict future events. Regression models are commonly used in finance, insurance and medicine. Regression modeling follows a rigorous process of evaluating suitability of the training data, evaluating data biases, discovering predictive variables, testing that correlations are better than random chance and evaluating the predictive accuracy of the final model.

Our model development and testing followed the ***Federal Reserve*** (Fed) and ***Office of the Comptroller of the Currency*** (OCC) supervisory guidance on model risk management: SR 11-7. The Fed and OCC issued this guidance because of the importance of forecasting models for the stability of the banking industry and to create a rigorous standard for developing and assessing models that could present significant risk. Our model is therefore suitable for banks and other financial institutions.

Our model is accurate and up-to-date, identifying just 0.4% of companies that represent 50% of reportable PII data breaches in the United States (a perfect model would identify 0.04% of companies—i.e. the exact companies that will experience data breach each year). Headcount information on companies is gathered two times per year.

Our data breach model was trained on the differences between all companies that did and did not experience a reportable PII data breach. We used breach notification letters from state attorneys generals from key states, as well as United States census data to generate a training data set that represents all companies in the United States.

We used probability of a reportable PII data breach because there is sufficient public data to develop accurate models due to ubiquitous reporting laws, and because probability of PII data breach is a good measure of cybersecurity overall. Cybersecurity encompasses much more than simply PII data breach, but in using the model we assume that the same security posture that reduces PII data breach also reduces other cybersecurity risks.

The data breaches forecast by our models are, all reportable PII data breaches such as those caused 1) by a **Malicious Outsider**, which can include network intrusion and infiltration of an email account; 2) by a **Malicious Insider**, which can include contractors, past employees and current employees; 3) by **Accidents** which can include emailing sensitive data to the wrong client or potential data exposure due to misconfiguration of an application or server; and 4) by unencrypted **Lost or Stolen electronic devices** including laptops, thumb drives and tape drives, misplaced, stolen or lost in transit.

About the Authors

Rick Lucas is the Managing Partner and CEO of GRN - Grand Rapids, a company that is focused on helping organizations acquiring top technical talent. He leverages his IT leadership as a former CIO to help organizations find the right talent to set up the organization for success and to ensure that IT departments are a partner for the business. He has received multiple awards from clients and employers for his leadership.

Thomas Lee is the CEO of VivoSecurity, a company focused on data collection, regression modeling and AI to quantify cyber security risk. Thomas has spoken at the Richmond Fed research conference 2018, invited participant at Richmond Fed cyber security workshop 2019, invited speaker at O.R.X Toronto & Milan 2018, speaker at OpRisk North America 2018, ACAMS panelist 2019, PRMIA NYC & BCG 2018, multiple patents for quantifying cyber security risk. Thomas holds degrees in Physics and Electrical Engineering from the University of Washington in Seattle, and an MS and PhD in Biophysics from the University of Chicago.