

# Case Study

## The Implicit Costs of Improper Security

A Business Impact Analysis, Supported By Cases Studies

### Abstract

Litigation. Fines. Lost Revenue. Share Price Decline. Customer Exodus. Incident Response. Brand Damage.

#### Improper security erodes the bottom line.

For progressive enterprises, security has evolved from an IT issue to a central business issue, as most companies today are responsible for protecting some form of digital asset, such as credit cards, customer data, business strategy, and intellectual property. As with all business concerns, cost management is of primary importance. With security, however, the true cost does not lie in a typical budget line item expenditure, but rather stems from asset compromise, which costs range from litigation, to fines, to lost revenue, to incident response. By contrast, however, proper hardening techniques are minimal expenditures in comparison, and are effective in dramatically reducing exposure to attack.

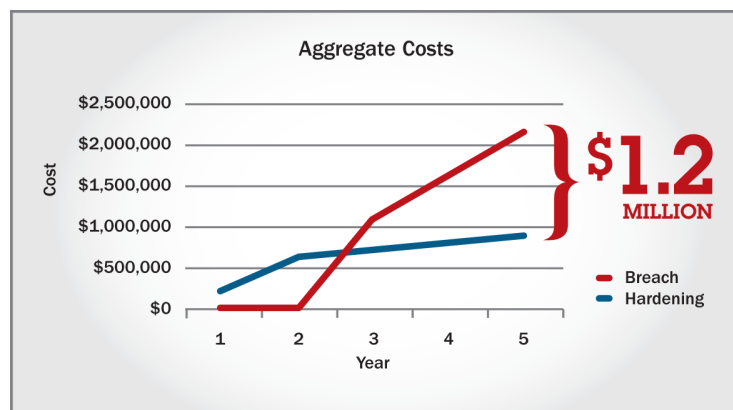
The challenge for many companies is to understand which hardening efforts are most effective. Studies<sup>1</sup> show that as many as 89% of CIOs express confidence in the effectiveness of their security practices, yet those practices often fail to account for evolved, modern adversaries. The black market<sup>2</sup> for stolen digital assets has matured, and sophisticated adversaries with financial motivations are incentivized to attack large companies who possess high value digital assets. When these adversaries are *unsuccessful*, incident response costs are significant – but when they are successful, the resulting damages skyrocket to staggering and potentially crippling heights.

Contained herein is an analysis of the different cost drivers as well as discussion of approaches to minimize exposure.

### Case Study: Incident Response

#### OVERVIEW & FINANCIAL IMPACT

ISE was recently engaged to investigate a security breach for a company who was the victim of a sophisticated, targeted attack. The victim company in question is a government contractor specializing in aerospace technology for the Department of Defense. What makes this case compelling is that the victim actually caught and stopped the attack before any assets had been exfiltrated, yet saw indirect damages incurring immediate costs over **\$578,000, plus** an additional **\$517,000/year** in additional spending moving forward.

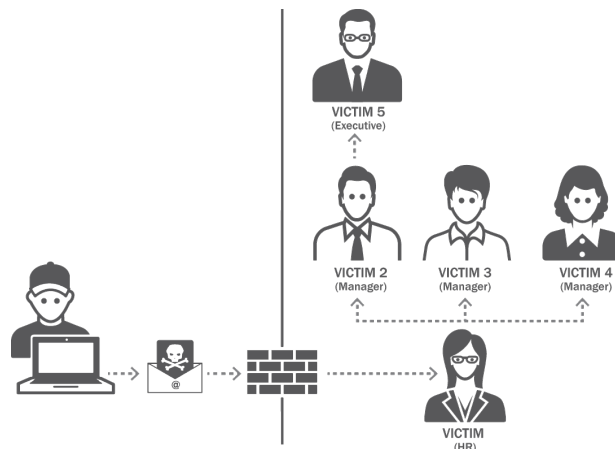


<sup>1</sup> Key Findings from the Global State of Information Security Survey 2014, Price Waterhouse Coopers. [www.pwc.com/security](http://www.pwc.com/security)

<sup>2</sup> [http://www.rand.org/content/dam/rand/pubs/research\\_reports/RR600/RR610/RAND\\_RR610.pdf](http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf)

## ATTACK ANATOMY

A threat actor (later determined to be an advanced persistent threat, a sophisticated adversary commonly referred to as APT) had responded to a job posting by the Accounting department of the victim company, with an attached resume that contained malware. The attack was both targeted (it addressed the victim individual by name, in response to a legitimate job posting by the company) and sophisticated (it delivered malware through spearfishing, and later attempted to phone home to a command and control server in an obfuscated, hidden way).



## ATTACK OUTCOME

The attack payload and delivery mechanism were very effective: The qualifications of the fictitious job applicant were fabricated to perfectly suit the needs of the open job position, and thus the resume was distributed internally, maximizing damage by delivering the attack payload whenever someone opened the malicious attachment. Upon investigation, it was determined that while the attack was successful in infecting several machines within the victim company's secure perimeter, no assets appeared to have yet been exfiltrated.

## REACTIONARY EXPENDITURES

Although no damages were directly related to data compromise, indirect expenditures were nevertheless incurred. Costs break into two categories:

### I. Response Costs [**\$578,000**]:

- [**\$122,000**] Consulting fees for investigation.
- [**\$240,000**] Resource investment by victim company's personnel to respond to findings from the investigation. Heavy involvement from executive leadership and C-suite contributed notably to cost ramifications.
- [**\$216,000**] Estimated lost opportunity costs, as victim's customer scaled back engagement for an extended period while the incident was investigated and remediated.

### II. Forward-looking Costs [**Additional \$517,000/year**]:

- [**\$138,000/year**] Additional security personnel in-house.
- [**\$165,000/year**] Expanded consulting contracts.
- [**\$214,000/year**] New, replaced or upgraded equipment and systems.

## COMPARISON: PREVENTATIVE HARDENING

Prior to the incident, the victim company relied heavily on automated scanning, had outdated systems deployed, was understaffed in the security department, and had not properly engaged outside resources to harden systems. Proper spending in these categories would have incurred an additional estimated **\$550,000** over 24 months, after which the company would have greatly reduced the likelihood of a successful attack, and been better prepared to respond to this attack.

## SUMMARY, PROJECTED SAVINGS & LESSONS LEARNED

The entire **\$550,000** expenditure to properly secure prior to an incident is surpassed by the **\$578,000** Response Costs alone, plus the extra **\$517,000/year** required for the additional services and equipment. In our estimation, had this company properly invested the appropriate security spending prior to the incident, they could have **saved** at least **\$1.2 million** over 5 years, all while being more secure.



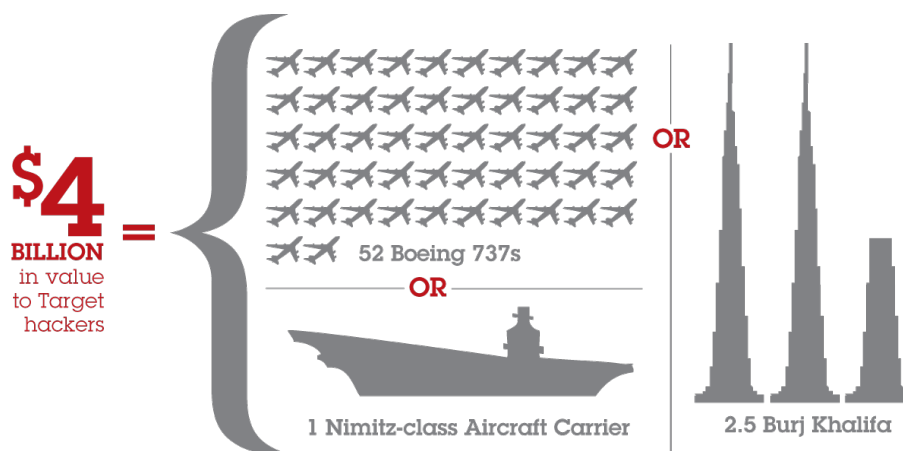
It is worth noting that these cost ramifications stem from an incident that did *not* result in stolen assets. Compromised assets would have exponentially multiplied the costs and damages, although the cost to properly defend those assets does not change either way.

## Case Study: Target Breach

### OVERVIEW & FINANCIAL IMPACT

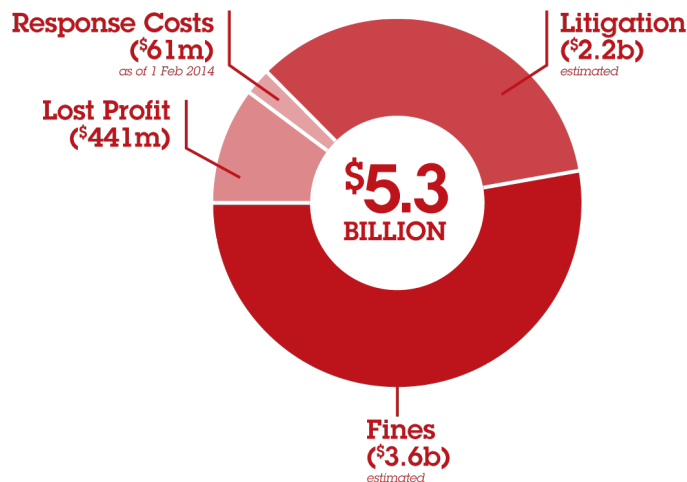
During the winter holiday shopping season in Q4 of 2013, cyber thieves broke into Target's network environment and stole approximately 40 million credit card numbers.

For the adversary the upside is massive. The total black market value for the stolen credit card information is estimated at between **\$800 million – 4 billion<sup>3</sup>**, based on the batch sale of credit card numbers, plus the yet-unknown scope of fraudulent purchases in the secondary black market resulting from the use of that stolen card information. This lucrative effort for the thieves is one that will undoubtedly embolden other criminals to pursue similar gains.

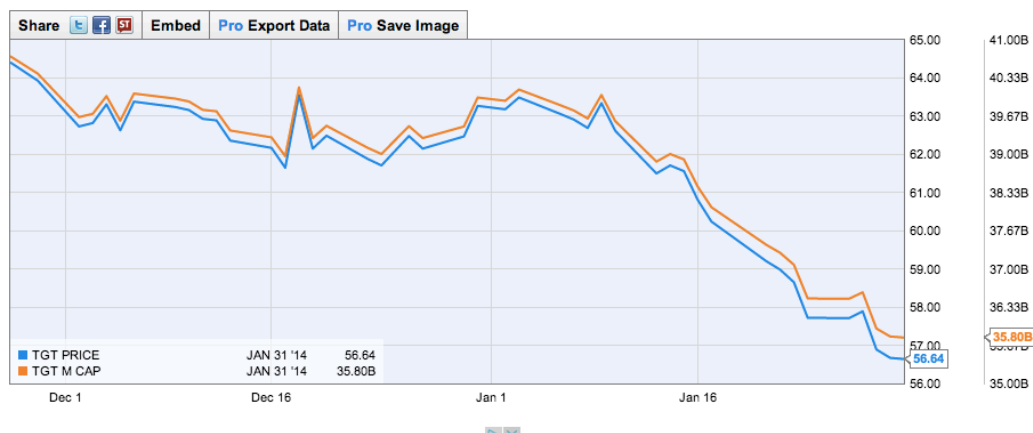


<sup>3</sup> The 40,000,000+ stolen cards are fetching \$20-100 per card, sold in batches of 1,000,000 cards on the black market. Source: [www.krebsonsecurity.com](http://www.krebsonsecurity.com).

For Target the downside is still unfolding, but damages could soar **over \$5.3 billion**. As of 1 Feb 2014, Target has already incurred **\$61 million**<sup>4</sup> in costs responding to the event. Furthermore, profit **fell 46%**<sup>5</sup>, or **\$441 million**<sup>6</sup>, as compared to the same period from the previous year. There are currently over **90 lawsuits** against Target (some even naming Target's security vendors<sup>7</sup> as defendants), from which experts expect damages to total between **\$1.4 billion to \$2.2 billion**<sup>8</sup>. In the likely event that Target is found to have been in non-compliance of Payment Card Industry (PCI) standards, Target will be liable for **\$90/cardholder**, or **\$3.6 billion**<sup>9</sup>.



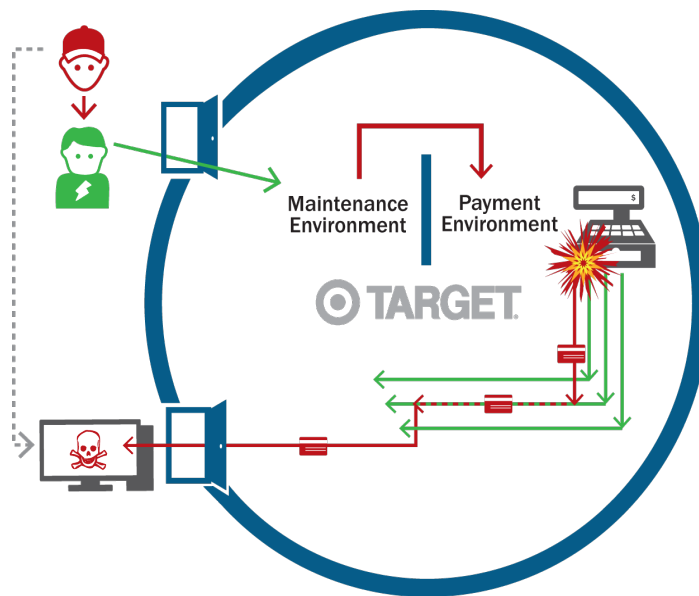
Over the period of 27 November 2013 to 1 February 2014, Target share price plummeted<sup>10</sup> **-12.1%** (from **\$64.41** down to **\$56.64**), which represented an overall market cap loss of nearly **\$5 billion** (from **\$40.71 billion** down to **\$35.80 billion**). According to investment analysis<sup>11</sup>, nearly every key investor metric at Target was down in Q4 2013, causing performance to fall short of projections: transaction count decreased **5.5%** (a rate surpassing even the **4.8%** decline at the peak of the 2008 financial crisis), sales decreased **3.8%**, and sales at stores open at least a year fell **2.5%**.



<sup>4</sup> Target investor report. <http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight=>  
<sup>5</sup> <http://online.wsj.com/news/articles/SB10001424052702304255604579406694182132568>  
<sup>6</sup> <http://www.cbsnews.com/news/data-breach-costs-take-toll-on-target-profit/>  
<sup>7</sup> <http://www.chicagobusiness.com/article/20140325/BLOGS11/140329865>  
<sup>8</sup> <http://www.bizjournals.com/twincities/news/2014/01/31/targets-breach-costs-billion-dollars.html>  
<sup>9</sup> <http://www.supermoney.com/2013/12/target-faces-potential-3-6-billion-liability-credit-card-breach/#.UriH-2RDtdE>  
<sup>10</sup> <http://www.ycharts.com>  
<sup>11</sup> <http://www.reuters.com/article/2014/02/26/us-target-results-idUSBREA1P0WC20140226>

## ATTACK ANATOMY

Target was the victim of a sophisticated, targeted attack that required high levels of skill, motivation and resources to accomplish. Utilizing a spear-phishing email campaign, attackers obtained the credentials of a trusted Target vendor, which they then used to remotely access Target's network environment. From there, they took advantage of improperly segmented networks to jump into the payment environment, install malware on the point of sale machines, and use the malware to extract decrypted credit card information from system memory.

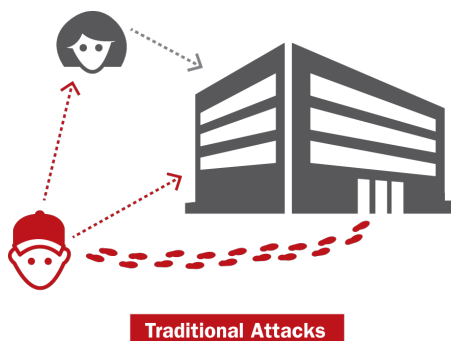


## ATTACK OUTCOME

Over the eighteen day period spanning 27 November and 15 December 2013, the thieves obtained over 40 million credit card numbers and an additional 70 million records containing customer information.

## SUMMARY & LESSONS LEARNED

The financial ramifications for Target are staggering, coming from all fronts: new security expenditures; legal damages; fines; income decline; and customer exodus. Yet, the entire attack stems from a fairly straightforward and solvable problem: defending against modern attacks requires hardening systems against attack vectors that originate from within trusted boundaries. Target was breached via a trusted vendor.



Traditional Attacks



Modern Attacks

Properly securing a digital supply chain, especially a complex one typical of large enterprises such as Target, is no easy task – but it *is* possible to dramatically reduce damage and decrease the likelihood of attack success. Hardening applications, infrastructures and the supply chain for Target is an effort that we estimate would cost in the **low single digit millions** – but in exchange would have saved what has already cost over **\$61 million** in response costs, plus **\$441 million** in lost Q4 income, plus further **yet-unknown billions** in possible punitive damages.

.....

**“Target would have paid very little attention to vendors like [the victim], and I would be surprised if there was ever even a basic security assessment done of those types of vendors by Target.”**

— *Target security manager*

.....

## Case Study: White Box vs. Black Box

---

### OVERVIEW

To improve the security posture of digital systems, progressive organizations engage third party security experts to calculate risk and provide hardening guidance. The most suitable approach is the **white box vulnerability assessment**. However, confusion about different security methodologies has led many IT executives to commonly request the notably ineffective approach of black box penetration testing. Most executives may be surprised to discover that this approach undermines the very risk assessment objectives they seek to achieve, while costing the same as or more than white box vulnerability assessments.



A major chipset manufacturer recently engaged ISE to assess the security of their newest secure chipset. The customer wanted ISE to perform a black box penetration test, which ISE did not believe would be appropriate given the circumstances (notably, that the customer was the creator of the target technology), favoring instead the far more valuable and effective white box approach. After many rounds of dialogue, the parties struck a compromise, agreeing to perform a black box penetration test first, followed by a white box vulnerability assessment. This provided a valuable case study to compare the financial and resource implications of the contrasting approaches.

### FINDINGS

The overall investigation was split into equal allocations of resources, first in a two (2) month session of black box penetration testing followed by a two (2) month session of white box vulnerability assessment. In the black box session, four (4) potential issues were identified, of which only one (1) was confirmed. No mitigation strategies were delivered, as we did not have knowledge about system architecture in order to intelligently suggest improvements. We were able to articulate only low confidence in project completeness, and were wholly unable to deliver a valid risk calculation.

In the white box session, we identified and confirmed eleven (11) critical issues, followed by another ten (10) severe issues. We were able to devise at least one (1) mitigation strategy for each of the twenty-one (21) confirmed vulner-

abilities. We had high confidence in project completeness and the risk calculation was of very high accuracy.

Both the black box and white box sessions were allocated the same resources, but the output of the white box portion was significantly more effective and valuable. Breaking the financial resource investment down to a per-issue value, this black box penetration test was found to require **22.2x more** resource investment, costing a staggering **\$55,000/issue identified**, as compared to a mere **\$2,475/issue identified** in the white box session that followed.

## Case Study: Chipset Manufacturer

	BLACK BOX	WHITE BOX
<b>Project Duration:</b>	2 months	2 months
<b>Resource Investment:</b>	200 hours	200 hours
<b>Critical Issues Identified:</b>	4 potential, 1 confirmed	11 confirmed
<b>Other Issues Identified:</b>	0	10 confirmed
<b>Mitigation Strategies:</b>	None	21+
<b>Risk Calculation Accuracy:</b>	Low	High
<b>Project Completeness:</b>	Unknown	Complete
<b>Cost Per Issue:</b>	<b>\$55,000</b>	<b>\$2,475</b>
<b>Cost Per Solution:</b>	Unknown, \$55,000	\$2,475

### ANALYSIS: PRICING

It is not straightforward to articulate which approach is more or less expensive, as pricing for both can be scaled up or down. The key difference lies in *how* each is scaled, and the impact that has on risk calculation. The cost for white box vulnerability assessment is related to system scope and project completion. In order to modulate pricing, evaluation components are added or omitted from scope. Although removing a component from an evaluation creates a blind spot, the blind spot is known and thus can be accounted for in the risk calculation.

By contrast, pricing for black box penetration testing is driven by effort input, irrespective of system scope or project completion. To modulate pricing, effort input is simply increased or decreased. However, blind spots in the evaluation remain largely unknown, and thus any risk calculation does not account for said blind spots and cannot make a risk determination with high confidence.

### ANALYSIS: EFFECTIVENESS

The results of a white box security assessment are of much higher value than that of a black box security assessment. When the system is fully understood by those performing the assessment, high confidence in the completeness of the job can be measured, assuring (or not) that most or all vulnerabilities have been identified, valid mitigation strategies have been recommended, and an accurate calculation of exposure risk has been delivered. By contrast, the results of a black box penetration test are of very low value: whether the security of the entire system has been addressed is unclear (if any issues are found it does not mean that all issues have been found, and conversely, if no issues are

found, it does not mean the system is secure), effective mitigation strategies may be difficult or even harmful to recommend, and very little can be determined about exposure risk.

In this case study, the white box approach uncovered substantially more security vulnerabilities, articulated valid mitigation strategies, and with high confidence calculated risk. The black box approach was summarily an ineffective use of time.



## SUMMARY & LESSONS LEARNED

Across industries, ISE has noticed a troubling preference for black box penetration testing and automated scanning in efforts to calculate risk and properly harden systems. Through both our consulting and research practices, we have found these approaches to both waste resources and be ineffective.

## Case Study: Manual Investigation vs. Automated Scanning

### OVERVIEW

Automated scanners were designed to be one of several tools in the toolbox of information security professionals. They are quick, cheap, and identify many basic issues. However, they have commonly become relied upon as the primary or even sole method of risk calculation and system hardening, something that such tools are not equipped to properly achieve. Organizations with valuable digital assets will attract sophisticated adversaries who will deploy targeted attacks to obtain those assets. Relying on automated scanning to defend against such motivated and skilled attackers will leave organizations vulnerable. Manual hardening, by contrast, is a tremendously thorough approach that uncovers not only common vulnerabilities but also uncommon ones, and especially those that would require multiple-stage attacks to deploy. For organizations with valuable assets to protect, manual hardening is the most appropriate approach to harden systems against sophisticated adversaries and targeted attacks.

	 Automated	 Manual
Targeted Attacks	X	✓
Sophisticated Adversaries	X	✓
High Value Assets	X	✓

### CASE STUDY: FILE TRANSFER SYSTEM

The media & entertainment industry relies on high powered systems to facilitate the transfer of very large digital assets between various sites and vendors throughout the production process. These pre-theatrical digital assets are often valued at **over \$1 billion**<sup>12</sup> and thus security is of paramount importance (at least to the content owners). As a result, studio vendors and the creators of these file transfer systems undergo frequent security testing – predominantly of the automated variety.

During mid-2013, one such prominent file transfer vendor underwent a security assessment by the security team of one of the Big Six<sup>13</sup> major studios. The studio’s security team used automated scans to check for common types of vulner-

<sup>12</sup> <http://boxofficemojo.com/alltime/world/>

<sup>13</sup> <http://ezinearticles.com/?The-Big-Six-Top-6-Major-Film-Studios-in-the-Movie-Business&id=1750590>



abilities, such as those outlined by the OWASP Top 10<sup>14</sup>, after which the studio concluded that the application suite was free of vulnerabilities. A report was submitted stating that the product passed security inspection, listing the categories evaluated and next to each displayed the definitive “PASS” result.

Shortly thereafter, ISE was engaged to perform a manual assessment of the same product suite. The manual assessment disproved the automated scan findings, identifying **twenty vulnerabilities** of which **fourteen** were **critical<sup>15</sup>** or **high severity**. Furthermore, these critical and high severity vulnerabilities were categorized under 9 of the same 10 categories indicated as “PASS” from the previous, automated assessment.

## **EFFECTIVENESS: AUTOMATED V. MANUAL**

Vulnerabilities discovered manually that a scanner *could* have detected if used properly, but didn't:

- Reflective cross-site scripting
- Cross-site request forgery
- Binary heap overflow
- SSH user account protected by weak password shared across all vendor servers

Vulnerabilities discovered manually that a scanner is incapable at detecting

- View and modify access controls for other companies
- Escalate user permissions
- De-escalate user permissions
- Access arbitrary media assets from different companies
- Login with another users client certificate
- Persistent cross-site scripting
- SSH port forwarding
- Unauthorized database access
- Arbitrary command execution

## **ANALYSIS: INDUSTRY TRENDS**

In an effort to analyze the trend preference for automated scanning at an industry level, ISE examined the audit history of the 8 highest priority<sup>16</sup> vendors in media & entertainment. Of these vendors, all 8 were actively in use by at least one of the Big Six studios, and most were in use by four or more. These vendors had previously been through substantial studio-required auditing, with a combined 160 audits<sup>17</sup> between them over the trailing five years. ISE did not have access to the methodology or findings of all 160 audits, but based on the sampling that were shared, combined with the studios', vendors', and past auditors' own claims, these assessments were predominantly automated. At that time, aside from prudent concern, the systems were largely considered to be secure.

Over the period 15 May 2012 through 15 November 2013 (18 months), we aggregated data related to ISE's manual security assessments of these same 8 vendors. Given that these systems were considered hardened and secure through past assessments, our findings were staggering:

- **120** total vulnerabilities
- **28 critical** severity vulnerabilities
- **34** high severity vulnerabilities
- **25** medium severity vulnerabilities
- **33** low/unknown severity vulnerabilities

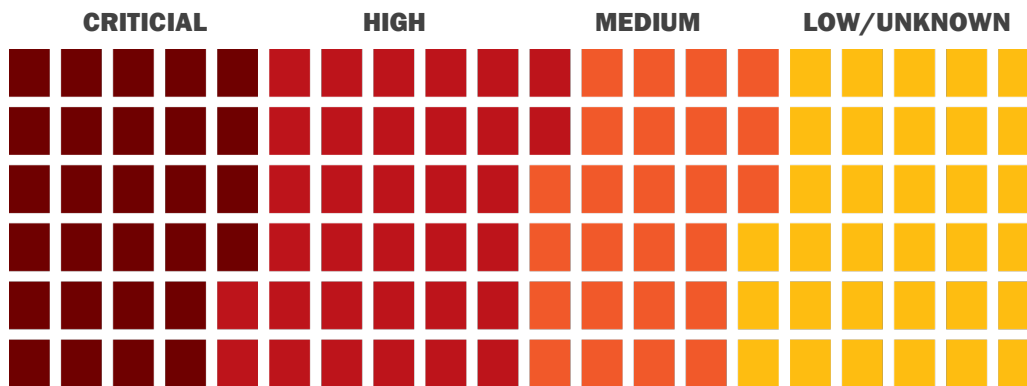
---

<sup>14</sup> [https://www.owasp.org/index.php/Top\\_10\\_2013-Top\\_10](https://www.owasp.org/index.php/Top_10_2013-Top_10)

<sup>15</sup> ISE considers a vulnerability critical if it is readily exploitable by an unsophisticated adversary with no preexisting access.

<sup>16</sup> “Highest priority” as defined by studio director(s) of content protection, regarding vendors that access, store, modify or transfer high value assets.

<sup>17</sup> Figure based on vendor-supplied estimates and anecdotal data.



### ANALYSIS: PRICING & RESOURCES

Automated scanning and code analysis is typically inexpensive, with annual licenses ranging from **free**<sup>18</sup> to the **double-digit thousands of dollars**<sup>19</sup>. Manual investigation is typically more expensive, with per-project fees ranging widely in the **tens of thousands of dollars**<sup>20</sup>, depending on size of system scope. Likewise, automated assessment is typically completed promptly and measured in minutes to hours, while manual assessment is measured in days or weeks.

Consider now that automated assessment, while requiring lower investments of cost and resources, is only effective at revealing the very lowest hanging fruit. Thus, only the weakest adversary is stopped. For some, this may be sufficient, but when allocating resources to any important cause, the effort should be related to the value of the cause – in this case, the value of the assets protected. If your assets are important, they should be treated as though they are important, and the appropriate diligence and resources devoted to their security.

Security professionals who rely on automated scanning often point to the low price point as the motivating benefit of using this approach. However, although manual investigation is more expensive than automated scanning, the difference is minor in comparison to asset value. Consider the fines related to a hypothetical breach of a system storing customer credit cards. Keep in mind that these metrics analyze just a single aspect of damages (fines), but there are many other areas of damage as well (incident response costs, litigation, revenue decline, etc):

Average number of cards stolen in recent high profile breaches <sup>21</sup> :	18,260,000
Fine per stolen card <sup>22</sup> :	\$90/each
Potential fine exposure of an average sized breach:	<b>\$1.643 billion</b>
Example cost range of automated scan:	\$5,000 - \$12,000
Example cost range of manual investigation:	\$40,000 - \$90,000
Example difference between approaches:	<b>\$35,000 - 78,000</b>
Percentage of cost difference vs. potential exposure:	<b>0.0047%</b>

### SUMMARY & LESSONS LEARNED

Although manual investigation is typically more expensive than automated scanning, the benefits far outweigh the cost delta, which is relatively insignificant in comparison to the potential damages of a breach. Manual investigation uncovers both commonly known and previously unknown vulnerabilities unique to the target system. Analyzing the data proves that even those organizations who take security seriously fail to properly secure systems when relying on automated scanning.

<sup>18</sup> <http://nmap.org>; [https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project); <http://www.metasploit.com>

<sup>19</sup> <https://store.tenable.com/>; <https://www.rapid7.com/products/nexpose/editions.jsp>

<sup>20</sup> Aggregated and anonymized data from ISE consulting practice 2005-2014.

<sup>21</sup> TJX (45.7m. 2007), Target (40m. 2013), Adobe (3m. 2013), Global Payment Systems (1.5m. 2012), Neiman Marcus (1.1m. 2013)

<sup>22</sup> <http://www.supermoney.com/2013/12/target-faces-potential-3-6-billion-liability-credit-card-breach/#.UriH-2RDtdE>

## About ISE

---

Founded in 2005 out of the PhD program at the elite Johns Hopkins' Information Security Institute, ISE is a sophisticated security consulting firm dedicated to aggressive defense strategies through advanced science. This select team of hackers, computer scientists, reverse engineers, and cryptographers helps companies harden systems against targeted attacks from sophisticated adversaries by utilizing a unique perspective typically perpetrated by the adversary.

ISE is most commonly recognized for being the first company to exploit the iPhone<sup>23</sup>, an achievement that garnered international attention. Other high profile compromises include ExxonMobil SpeedPass, Texas Instruments RFID, Diebold eVoting Machines, and numerous others. ISE's most recent research discovered systemic issues in SOHO routers<sup>24</sup> and web browsers<sup>25</sup>.

Executives and analysts from ISE are sought-after thought leaders, speaking at events across the country and around the world, including at prestigious events such as DEFCON, BlackHat, South by Southwest (SXSW), Content Protection Summit (CPS), National Association of Broadcasters (NAB), Healthcare Information and Management Systems Society (HIMSS), and Hotel Technology Next Generation (HTNG), amongst many others.

---

<sup>23</sup> [http://www.nytimes.com/2007/07/23/technology/23iphone.html?\\_r=2&](http://www.nytimes.com/2007/07/23/technology/23iphone.html?_r=2&)

<sup>24</sup> [http://securityevaluators.com/content/case-studies/routers/soho\\_router\\_hacks.jsp](http://securityevaluators.com/content/case-studies/routers/soho_router_hacks.jsp)

<sup>25</sup> <http://securityevaluators.com/content/case-studies/caching/index.jsp>