SURVEY REPORT

2016 Pre-Holiday Retail Cyber Risk Report

An Osterman Research Survey Report

Published November 2016

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

You would expect cyber security to be a number one issue on retailers' minds, particularly during the holiday season, due to a confluence of factors:

- The number of temporary employees increases dramatically during the holiday season as retailers hire staff primarily for retail floor operations. The National Retail Federation estimates that 640,000 to 690,000 people will be hired during the 2016 Holiday season[i].

- These employees may have access to sensitive and confidential information, such as customers' financial and personal information.

- Retail systems are stressed during the holidays, since the 61-day holiday season represents less than 17 percent of total shopping days in 2016, but as much as 27 percent of some retailers' sales[ii].

However, during October 2016, Osterman Research conducted a second annual survey on the behalf of Bay Dynamics that revealed a new twist: The majority of IT and security professionals that manage retailers' cyber security programs do not feel more pressure during the holiday season to protect their organization's data.

ABOUT THE SURVEY

In October 2016, Osterman Research conducted a survey on the behalf of Bay Dynamics to understand the cyber security and risk issues IT and security professionals in retail organizations face when trying to protect their organizations, particularly during the holiday season. This survey was similar to one conducted by Osterman Research during late 2015, making some of the data comparable.

The October 2016 survey was distributed to 134 IT and security professionals in large, retail organizations operating in the United States. To qualify for inclusion in the survey, individuals had to be involved in the management of their organizations' IT and security systems, and had to work for a retail organization of at least 2,000 employees.

KEY TAKEAWAYS

Some of the key takeaways from the research conducted for this report include:

- **Cyber security is no longer a "seasonal" priority**
  IT and security professionals say they feel pressure year-round to secure their organizations, not just during the holidays, vs. in 2015 when a majority said they felt more pressure during the holidays to secure their organizations. IT and security professionals are seeing a persistent cyber threat. They understand they can get hacked or suffer a breach any day of the year. Therefore, they are under pressure all the time, not just during the holidays.

- **Vulnerabilities are being patched more quickly**
  Because cyber security is now a year-round commitment for IT and security professionals, they are addressing vulnerabilities more quickly, with almost 60 percent saying they patch within 48 hours of discovering the vulnerability.

- **Employees are being watched more closely**
  There has been a four-fold jump between 2015 and 2016 in the number of IT and security professionals who say their permanent employees have accessed and/or sent sensitive data they should not have accessed and/or sent. There has also been a significant decrease in the number of IT and security professionals who say they are not sure if their permanent employees have accessed and/or sent sensitive data they should not have accessed and/or sent. The results show IT and security teams have a better understanding of what's going on in their environment.

- **Access to sensitive, personal information is limited**
  Only six percent of IT and security professionals say their temporary employees have access to personally identifiable information (PII), and only 13 percent say their contractors can access PII. The findings show retailers are limiting access to their most sensitive information, which greatly helps reduce the risk of that information being compromised.

- **Temporary employees do not get their own accounts, but also have limited access**
  The majority (64 percent) of IT and security professionals say they don't give temporary employees their own accounts, and therefore they also don't give them access to sensitive data. For those who say they do (36 percent) give temporary employees their own accounts, they are also doing a better job monitoring those employees. For example, only 12 percent of respondents say they have little to no visibility into what they temporary employees are doing on the network.

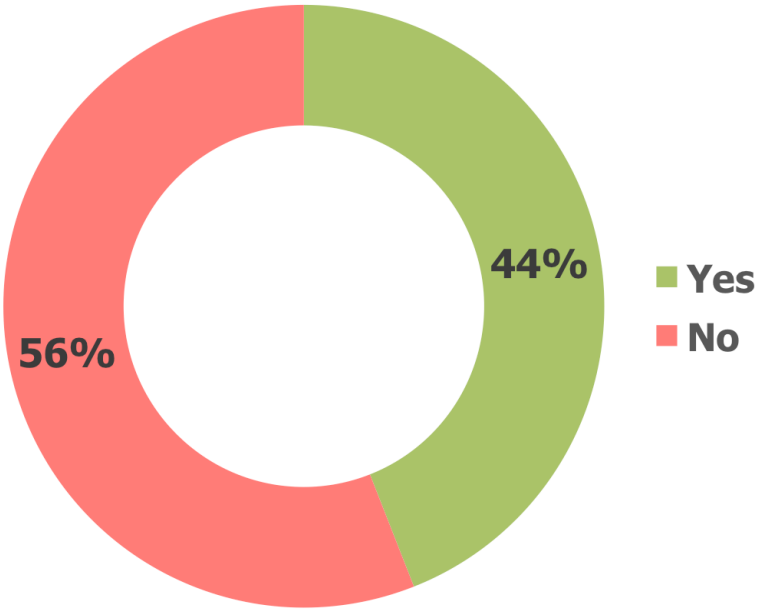
- **Security awareness training is a one-time happening**
  Only eight percent of IT and security professionals say their companies provide security awareness training after a security problem has occurred. Most companies tend to do annual security awareness training or when employees first join a company. It's a wide-sweeping, multi-hour training session that covers just about everything cyber security. That is not as effective as targeted training that focuses on individual policies that have been violated and the employees who violated them.

SURVEY FINDINGS

CYBER SECURITY IS NO LONGER SEASONAL

The majority (56 percent) of IT and security professionals say they do not feel more pressure during the holidays to protect corporate data, as shown in Figure 1.

Figure 1
"Is there more pressure on your IT/security team during the holidays to protect your organization's data?"



Source: Osterman Research, Inc.

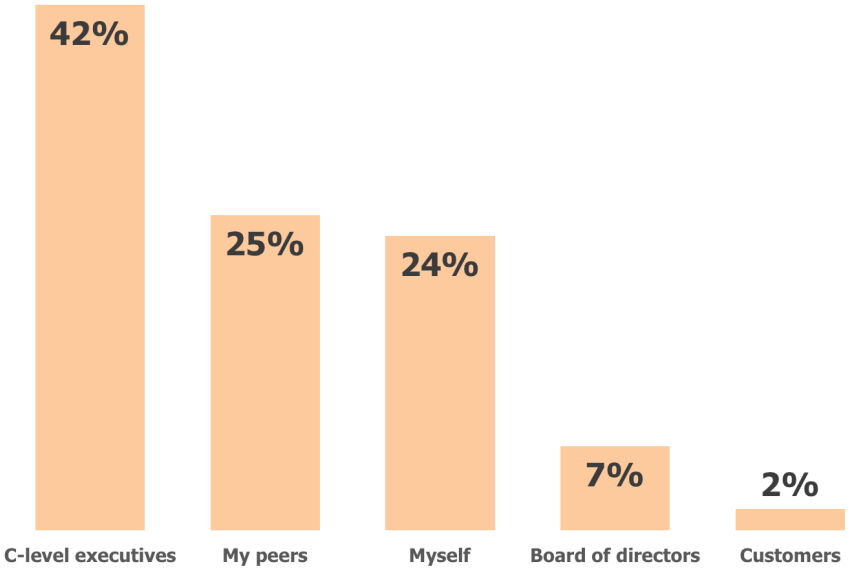
The results indicate that IT and security professionals feel pressure year-round to secure their organizations, not just during the holidays. This is in stark contrast to the survey we conducted in 2015, which found the majority (66 percent) of respondents said they felt more pressure during the holidays to secure their organizations. IT and security professionals are seeing a persistent cyber threat. They understand they can get hacked or suffer a breach any day of the year. Therefore, they are under pressure all the time, not just during the holidays.

And, based on other industry research, the continuous pressure is well founded. A 2014 KPMG survey of 1,400 U.S. consumers found that more than one-quarter of them would refuse to shop at a store that had experienced a data breach unless the product they sought was available nowhere else[iii]. The survey also found that roughly three in five consumers lacked confidence in, or at least were unsure of, the security of their information at both online and brick-and-mortar retailers[iv].

WHERE DOES THE PRESSURE COME FROM?

For those IT and security professionals that feel more pressure during the holidays to protect their organization's data, much of the pressure is coming from the C-suite. As shown in Figure 2, more than two in five IT and security professionals who feel more security-related pressure around the holidays tell us their C-level executives are putting pressure on them, while 25 percent are feeling pressure from their peers and another 24 percent are putting pressure on themselves. Interestingly, IT and security professionals say boards of directors and customers are rarely pressuring them to do a better job securing their companies.

Figure 2
Primary Sources of Cyber Security Pressure Applied to IT and Security Teams



Source: Osterman Research, Inc.

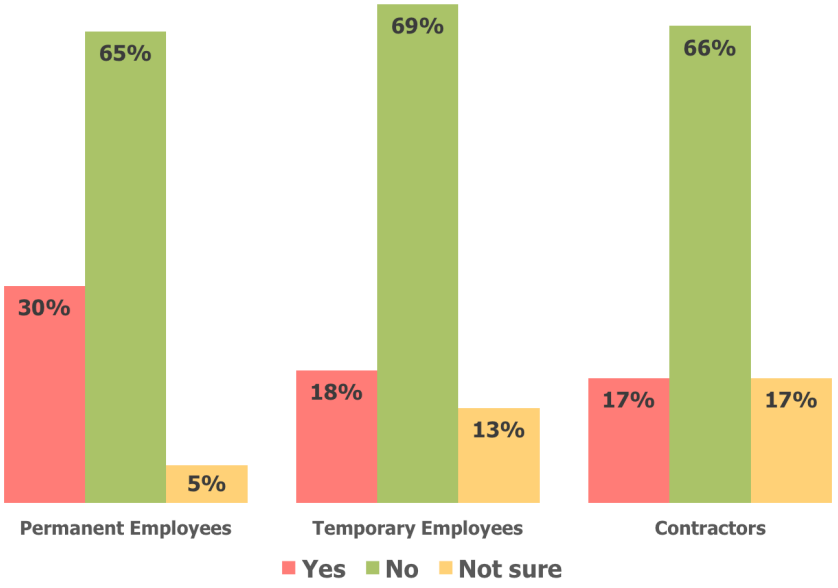
This data is interesting because it tells us that C-level executives are quite focused on security-related issues and are pressuring many IT and security professionals to do a better job at protecting corporate information assets. It also reveals boards of directors are not *directly* pressuring IT and security professionals to focus more on security around the holidays, but this pressure may be indirect. Recent surveys of boards of directors conducted by Osterman Research have found that board members are becoming more security-conscious and involved in cyber security

decisions. We suspect they are pressuring senior executives in their companies to do a better job at bolstering information security and, in turn, these executives are redirecting that attention to IT and security professionals.

EMPLOYEES ACCESS AND/OR SEND SENSITIVE DATA THEY SHOULD NOT BE ACCESSING

Our research found that every type of employee within a retail organization – permanent, temporary and contractors – have accessed and/or sent sensitive information in violation of corporate policy or legal requirements, as shown in Figure 3. A third of IT and security professionals say their permanent employees violated policies, surpassing the number of respondents who say their temporary and contractors violated policies. However, the results show each employee type has accessed and/or sent sensitive data they should not have accessed/sent at some point.

Figure 3
"Have any of your employees ever accessed and/or sent sensitive data they should not have accessed or sent?"



Source: Osterman Research, Inc.

There are a couple of interesting points in the figure above:

- In our 2015 retail survey, just seven percent of IT and security professionals said their permanent employees accessed and/or sent sensitive data they should not have accessed and/or sent; in the 2016 survey, 30 percent of respondents say their permanent employees have done so. That represents more than a four-fold increase in the number of respondents who say their permanent employees have accessed and/or sent sensitive data they should not have accessed and/or sent.

- The "not sure" number regarding permanent employees also decreased from 14 percent in 2015 to just five percent in 2016.

- These two data points lead us to conclude that IT and security professionals are more aware of employees sending out and accessing sensitive data they should not be sending out and/or accessing. In 2015, they were eyes wide shut; they didn't see sensitive data being sent out so they assumed it didn't happen. The bump in the number of respondents who say their permanent employees

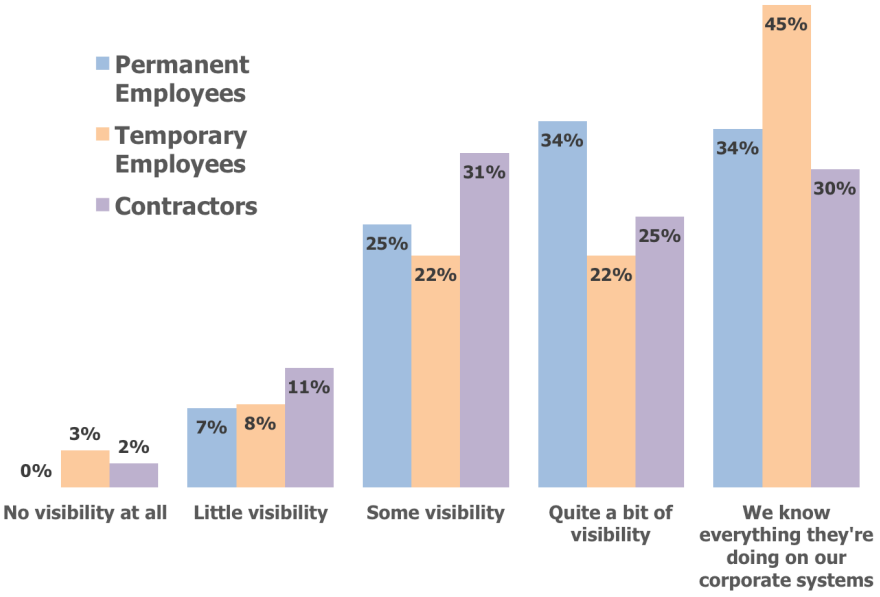
accessed and/or sent sensitive data they should not have accessed, coupled with the decrease in the "not sure" responses, show that IT and security professionals have a better understanding of what's going on in their environment, even though the percentages are still too low.

- Also, while more respondents say permanent employees violated policies by accessing or sending sensitive data improperly, the much higher proportion of permanent employees in most retail organizations means that permanent employees are less of a problem than either temporary or contract employees in the context of data breaches. For example, as of October 2016, there were just under 16 million retail workers in the United States[v]. If we assume that 690,000 temporary retail employees will be added during the 2016 holiday season, that means that temporary employees will account for only 4.3 percent of the retail workforce during the 2016 holiday season, yet they are responsible for 60 percent as many data breaches as their permanent counterparts.

IT AND SECURITY HAVE SOME VISIBILITY

Further validating our previous conclusion, as shown in Figure 4, a small percentage of IT and security professionals say they have little to no visibility into the behavior of their permanent employees. A majority say they have some level of visibility into the activities of all three types of employees – permanent, temporary and contractors.

Figure 4
"How much visibility does your IT and security organization have into the behavior of your employees when accessing corporate systems, customer data, and other sensitive data assets?"



Source: Osterman Research, Inc.

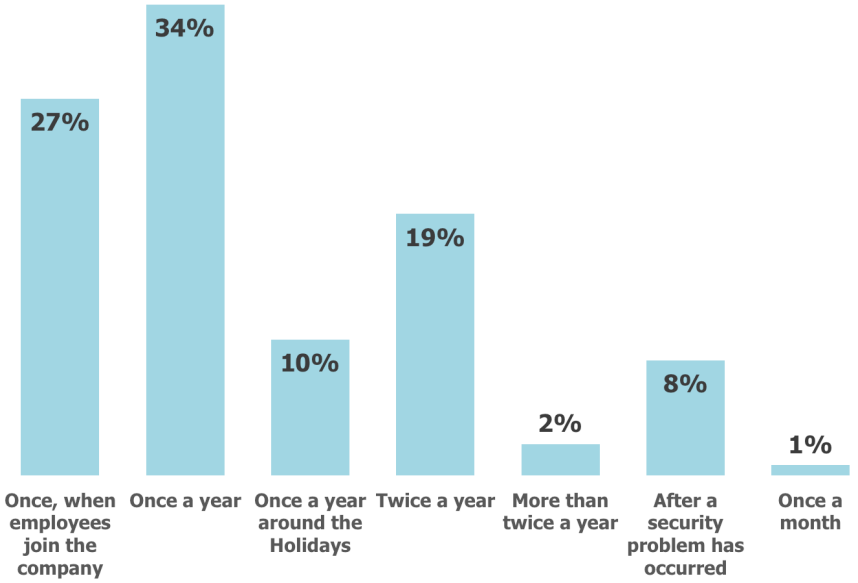
Interestingly, a plurality of IT and security professionals (45 percent) say they know everything their temporary employees are doing, but less about their permanent employees and contractors. This may be attributable to the fact, as discussed later in this report, that temporary employees are given the least access to valued systems and data.

THE IMPORTANCE OF SECURITY AWARENESS TRAINING

As shown in Figures 5 and 6, the majority of IT and security professionals say their permanent and contract employees receive security awareness training no more than once per year. Only a tiny proportion of employees receive more frequent training on key security issues. We believe this is part of the cyber security problem. Companies tend to do annual security awareness training or when employees first join a company. It's a wide-sweeping, multi-hour training session that covers just about everything cyber security. That is not effective. While a general overview once a year is helpful, companies also need targeted security awareness training that specifically focuses on individuals who violated security policies and speaks to the policy they violated. Bay Dynamics has seen an 80 percent drop in non-malicious behavior after this kind of targeted training.

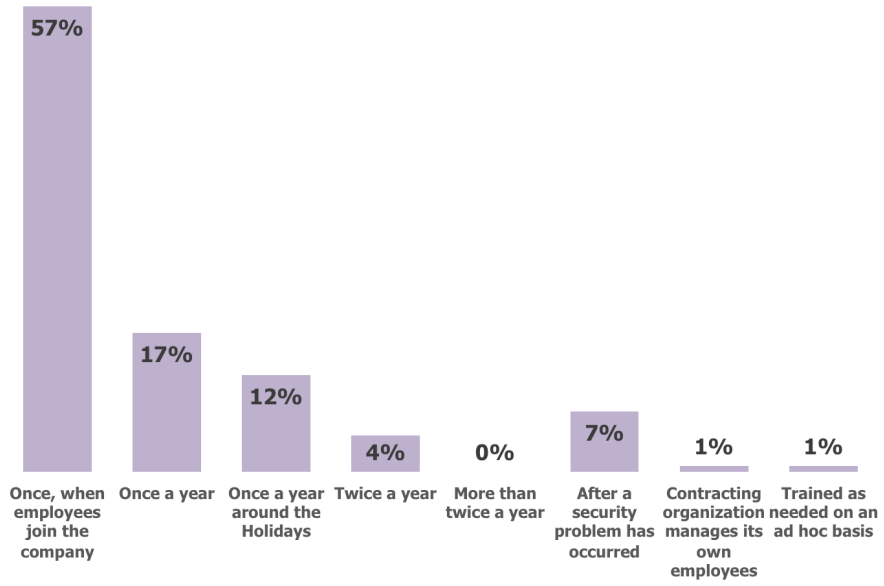
Separate research conducted by Osterman Research earlier in 2016 found that organizations that provide security awareness training at least once per year are 75 percent less likely to experience security problems than organizations that provide this training less frequently or not at all.

Figure 5
Frequency of Security Awareness Training for Permanent Employees



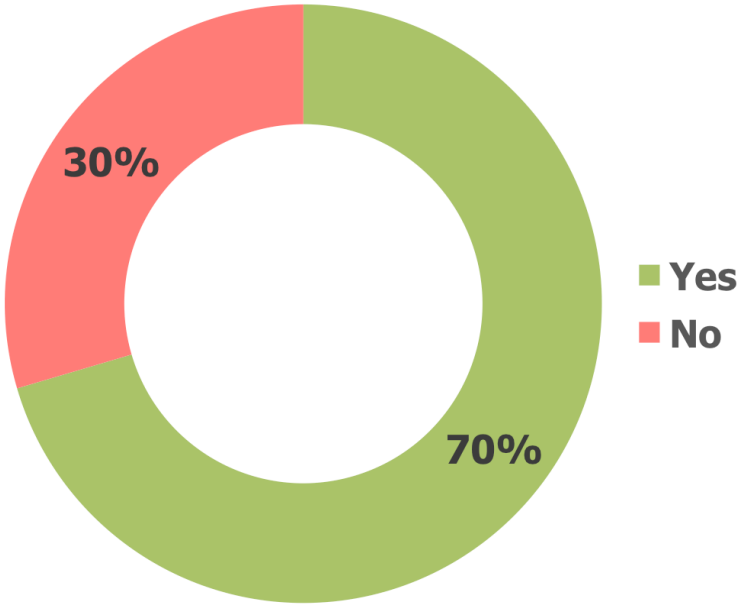
Source: Osterman Research, Inc.

Figure 6
Frequency of Security Awareness Training for Contractors



Source: Osterman Research, Inc.

Figure 7
"Do holiday temporary employees go through security awareness training?"

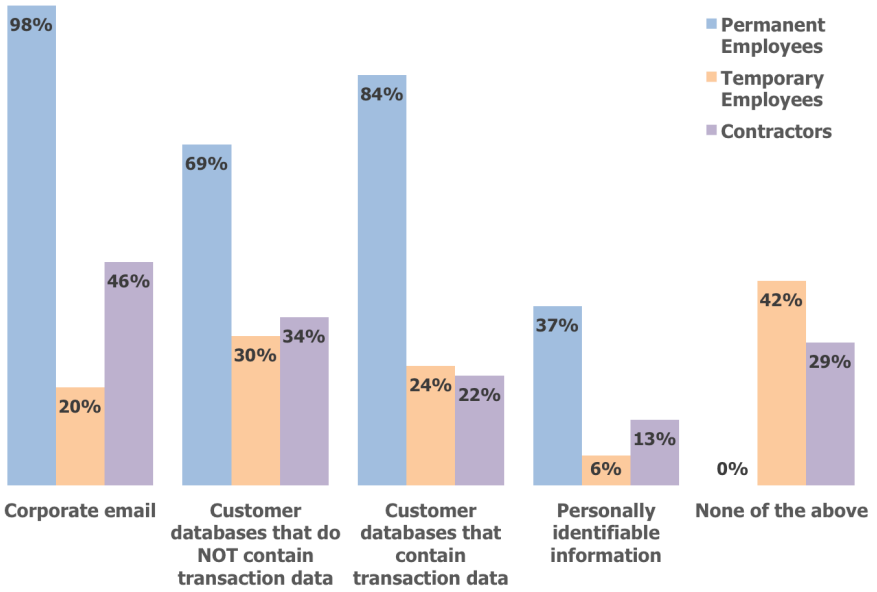


Source: Osterman Research, Inc.

OWN ACCOUNTS = MORE ACCESS = MORE MONITORING

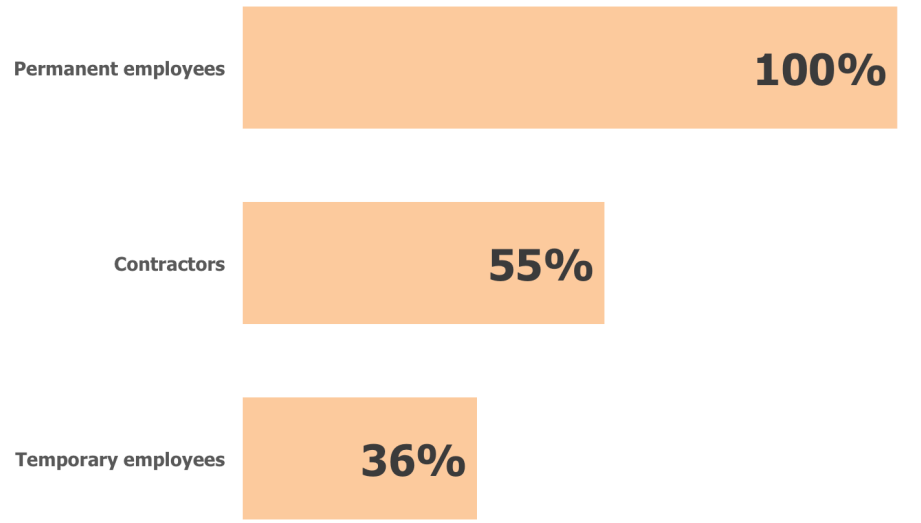
The biggest security problems in many organizations are not hackers, malware or vulnerable systems. Instead, the biggest problems are the people who have access to corporate systems and sensitive data. As shown in Figure 8, a clear majority of IT and security professionals say that permanent employees have access to corporate email or sensitive information, while some respondents say temporary and contract employees do as well. As shown in Figure 9, all IT and security professionals say permanent employees receive unique login credentials for corporate systems. A little more than half say contractors receive unique login credentials, and more than one-third say temporary employees receive unique login credentials for corporate systems.

Figure 8
Types of Data to Which Employees Have Access



Source: Osterman Research, Inc.

Figure 9
Employees That Receive Unique Login Credentials for Corporate Systems



Source: Osterman Research, Inc.

There are two important groups here:

- **Organizations that do not give temporary employees unique accounts**
  The majority (64 percent) of IT and security professionals don't give temporary workers their own accounts, and don't give them access to sensitive data. For example, six percent of respondents say their temporary workers access PII; 20 percent say they give temporary workers access to corporate email; and 24 percent say they give temporary workers access to customer transaction data. Overall, 55 percent say they don't give their temporary workers access to anything. Out of the respondents in this group that say they do not give their temporary workers their own accounts, 58 percent say they don't give their temporary workers access to email, sensitive databases or PII. That's a positive finding. If temporary workers don't have their own accounts, they should not have access to sensitive data. While there is still a pocket of IT and security professionals who are being unsafe, the majority have woken up. They realize that if their employees are using shared accounts, meaning they do not have their own unique login credentials, they should not have access to sensitive data.

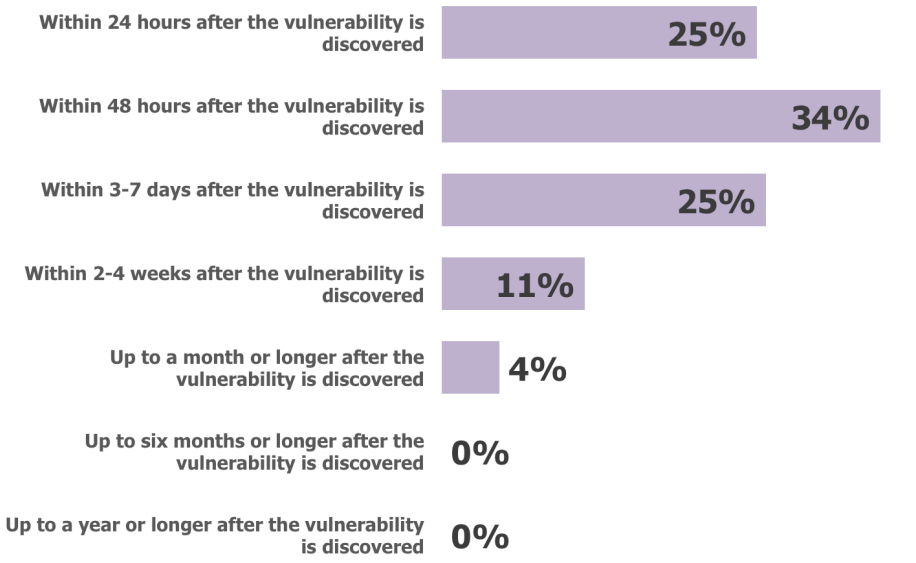
- **Organizations that do give temporary employees unique accounts**
  The second group is those IT and security professionals who do give temporary workers their own accounts. For those who do (36 percent), and give temporary workers access to PII, corporate email and customer transaction data (50 percent), they are also doing a better job monitoring those employees. Only 12 percent of respondents say they have little to no visibility into what their temporary workers are doing on the network.

SYSTEMS AND APPLICATIONS ARE BEING PATCHED MORE QUICKLY

Another positive finding from our research pertains to patching vulnerabilities. As shown in Figure 10, three out of five of the IT and security professionals we surveyed say they patch vulnerabilities in high value systems and applications within 48 hours after the need to patch them is identified. Another 25 percent of respondents say they take anywhere from three to seven days to patch these critical systems, while the remaining 15 percent say they take several weeks to do so. For that 15 percent, this is a serious issue, since the U.S. Department of Homeland Security estimates that nine out of 10 security incidents are the result of vulnerabilities in software[vi].

However, these numbers also indicate the shift in mindset of security being a year-round commitment. IT and security practitioners are patching systems and applications more quickly. They are more on top of the ball.

Figure 10
Time Taken for Patching Vulnerabilities in High Value Systems and Applications



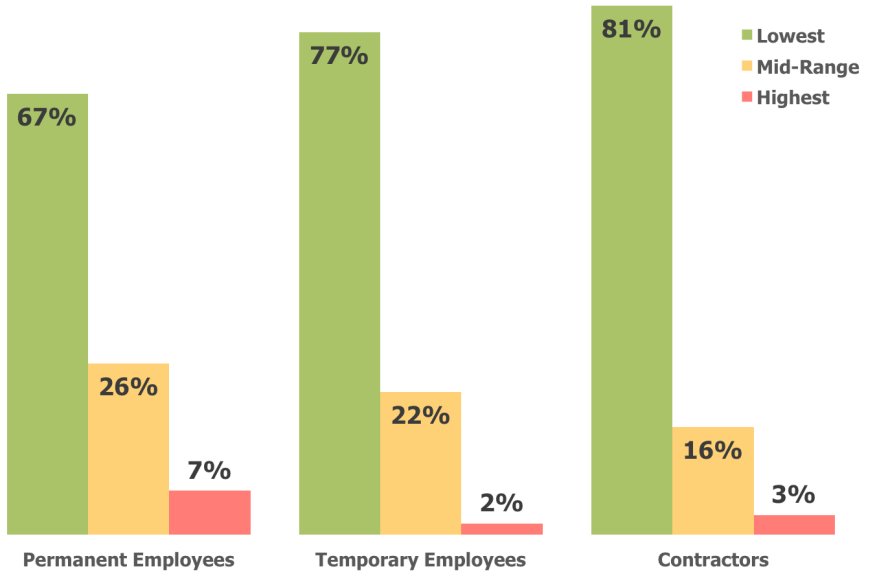
Source: Osterman Research, Inc.

Overall, the good news is that most organizations are quick to address known vulnerabilities in their critical systems. The bad news is a) that too many are still slow to apply these patches, and b) that vulnerabilities can exist for long periods before they are addressed. While one-quarter of organizations will patch vulnerabilities within 24 hours after they are discovered, it might take weeks or months to discover the vulnerability in the first place. For example, the Heartbleed vulnerability was introduced into the OpenSSL cryptography library in late 2011, became widespread in March 2012, but was disclosed publicly more than two years later in April 2014[vii].

MOST EMPLOYEES ARE NOT A SECURITY RISK…BUT

We also wanted to discover the extent to which IT and security professionals view employees as a security risk in the context of the cyber security violations they have committed. As shown in Figure 11, IT and security professionals say permanent, temporary and contract employees have a history of fairly minimal levels of security violations. However, seven percent of IT and security professionals surveyed tell us that permanent employees represent a high level of risk based on their past behavior of violating cyber security policies, while another 26 percent say their permanent employees represent a "mid-range" level of risk. Interestingly, an overwhelming majority of IT and security professionals say their contractors represent a low level of risk based on their past behavior of violating cyber security policies. Considering that in many of the retail breaches that made headlines during the past four years criminals' initial point of entry was through a third party contractor, this statistic is surprising.

Figure 11
Risk of Cyber Security Policy Violations by Employee Group



Source: Osterman Research, Inc.

CONCLUSION

The bottom line is that cyber security is no longer a seasonal responsibility. IT and security professionals in the retail space feel pressure to secure their organizations all year-round. They are in better control of their environments, especially regarding their temporary employees and what they can access. Either they don't give temporary employees their own accounts and therefore don't give them access to sensitive data, or they do give them their own accounts, access to sensitive data and they monitor them more closely. Fewer respondents are saying they give their temporary employees access to sensitive data and don't monitor them. That's a pervasive trend.

The key to reducing cyber risk within retail and other enterprise organizations is to focus on the most valued systems and applications. Organizations should identify where their most valued assets exist, who accesses them, how they access them and who governs those assets. They should then prioritize the patching of vulnerabilities based on the value of the asset at risk and associated threats to that asset. They should prioritize threats, both insider and external, based on the value of the asset at risk and additional business context, such as whether an employee's behavior was business justified.

No matter the types of employee, whether they are permanent, temporary or contractors, only those who must access valued assets to do their jobs should be given access. And, those who are given access must have unique login credentials and be monitored. In today's enterprise environment where manpower and resources are limited, the most effective way to reduce cyber risk is by focusing on the most valued assets and the people who interact with them.

ABOUT BAY DYNAMICS

Bay Dynamics® enables enterprises to prioritize security activities and direct their limited resources at their most important problems. The company's flagship product, Risk Fabric®, is a software platform for enterprises requiring timely prioritization and remediation of security exposures impacting their most critical IT systems and data assets. Risk Fabric benefits enterprises with improved timeliness of action by automating the delivery of personalized and prioritized vulnerabilities to line-of-business application owners responsible for remediation. The platform also enables enterprises to reduce costs and regulatory risk, fortify business continuity, and improve decision making by combining security tool data with business context to provide a complete view of risk mapped to valued assets. For more information, please visit www.baydynamics.com.

REFERENCES

[i] https://nrf.com/resources/holiday-headquarters/holiday-faqs
[ii] https://nrf.com/resources/holiday-headquarters/holiday-faqs
[iii] http://www.forbes.com/sites/barbarathau/2014/12/04/study-credit-card-breach-fears-haunt-consumers-holiday-shopping-plans/#2bfe1cd64b09
[iv] http://www.forbes.com/sites/barbarathau/2014/12/04/study-credit-card-breach-fears-haunt-consumers-holiday-shopping-plans/#2bfe1cd64b09
[v] http://www.bls.gov/iag/tgs/iag44-45.htm
[vi] http://www.csoonline.com/article/2978858/application-security/is-poor-software-development-the-biggest-cyber-threat.html
[vii] https://en.wikipedia.org/wiki/Heartbleed