FINTECH LAW REPORT
E-Banking, Payments & Commerce in the Mobile World

Nov/Dec 2014 ■ Volume 17 ■ Issue 6

Cybersecurity: *The Human Factor*

BY CHRISTOPHER AVERY & GWEN FANGER

Christopher Avery is a privacy and data security attorney in the New York City office of Davis Wright Tremaine LLP. Mr. Avery has nine years of in-house experience and regularly counsels companies on how to prepare for, respond to and recover from cybersecurity events. Gwen Fanger devotes her practice to commercial litigation and business counseling in the San Francisco office of Davis Wright Tremaine. She has more than eight years of federal enforcement experience as a Federal Trade Commission attorney, which enables her to advise clients in a range of compliance matters such as antitrust, UDAAP, mergers and acquisitions, and unfair business practices. Contact: christopheravery@dwt.com or gwenfanger@dwt.com.

Financial institutions are under a constant and growing cyber assault from hacktivists that want to cause online mischief, criminals that want to steal consumer data and nation-states that are looking for a military, political or economic advantage. In this increasingly costly war, the focus is often on the latest hardware, software and analytics to fortify the defenses. While technical security controls are an essential weapon in the arsenal, organizations should re-double their attention on the weakest link in their security suit of armor—their people. This article explores the human side of cyber defenses, including both a look at the inadvertent human errors and administrative failures that have contributed to some of the most significant cyber events and how administrative controls are weaved into the recently released *Cybersecurity Framework*.[1] Finally, this article offers some practical advice on how to improve the security posture of financial organizations with an increased focus on the "human element" and its role in cybersecurity.

Weaknesses in cybersecurity have had a significant impact on the financial services sector. It has been reported that the financial service sector suffered more than one-third of all security incidents with confirmed data losses.[2] The apparent targeting of this sector means that financial institutions cannot afford simply to focus on the threats from external parties and malicious insiders in their efforts to protect against data security breaches. They also must acknowledge and account for the behavior of their own internal employees and personnel in protecting sensitive organizational and consumer information. Indeed, a financial institution's trusted insiders are the organization's most valuable asset and, with increasing frequency, its weakest security link in data security. Given the amount of social media, the widespread sharing of personal information, and basic human nature that errs on the side of convenience and ease of operation, insiders effectively act as a human sieve that is challenging to plug even

CONTINUED ON PAGE 3

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, USA (978) 750-8400; fax (978) 646-8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651)687-7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

For subscription information, please contact the publisher at: west.legalworkspublications@thomson.com

Editorial Board

Fintech Law Report

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ■ 6 Issues ■ $752.04
(ISSN#: XXXX)

For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, USA (978) 750-8400; fax (978) 646-8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651) 687-7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered. However, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

CONTINUED FROM PAGE 1

with the most high-tech security. As a result, employees, contractors, and vendors increasingly represent potential entry points for cyberattacks. However, that could be mitigated by accounting for the realities of human behavior and focusing on the function of internal employees and related personnel when implementing administrative security controls.

Who Are the Insiders and What Threat Do They Pose?

"Insiders" include current or former employees, contractors or other vendors and service providers that an institution allows on its premises or access to its computing resources for legitimate, business purposes. They also include anyone allowed to establish a trusted connection from outside of an institution's parameters or control. Given the broad spectrum of those who an institution allows access but often has different levels of control over, risks arise with respect to creating and enforcing security measures that protect against the failings of basic human nature in these non-malicious insiders. Ultimately, no matter how much infrastructure or technology a company invests in, it is only as strong as its own people who are the first (and arguably most important) level of defense against the more routine, basic cyberattacks on financial institutions and other businesses.

The burden to protect consumer and financial data falls squarely on the shoulders of the institution that collects or maintains such data. This responsibility is substantial and can be exceedingly expensive both in the cost of creating and maintaining an infrastructure and data security program and also in paying for damages after a breach occurs. The Ponemon Institute's *2014 Cost of Data Breach Study* found that the average cost for each lost or stolen record containing sensitive information was $201 per record.[3] The federal government expects businesses to bear this expense and implement "reasonable" data security measures to protect the information. The challenge, however, is to provide adequate security given the variable that businesses cannot simply pay money to fix—human behavior.[4] Thus, the issue arises as to whether "reasonable" security measures now must include some effort to address weaknesses in human behavior among insiders.

For example, the Federal Trade Commission (FTC), which enforces consumer protection laws, investigates privacy breaches to determine "whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities."[5] The FTC's standard does not expressly mandate certain elementary security conditions—such as password requirements—but failure to do so likely would raise concern. By way of illustration, the FTC obtained a consent order against a retailer arising from a data breach affecting tens of millions of payment cards for failure to "provide reasonable and approximate security for personal information on its networks" where it, among other things, "did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks."[6] A security program that did not include specific measures that would help mitigate human error would unlikely be considered "reasonable" in light of a resulting breach.

Other recent data breaches illustrate how attackers continue to benefit from a company's own insiders' weaknesses, particularly employees and third-party vendors. Insider behavior—even if inadvertent—puts companies at risk from even unsophisticated plots to steal financial and consumer information.

Unauthorized employee access to or use of information has contributed a number of recent data security breaches. For example, AT&T Inc. recently informed consumers that it had encountered a data breach last August affecting about 1,600 customers.[7] AT&T disclosed that an employee had improperly accessed customer data and may have obtained account information, including driver's license and Social Security numbers.[8]

Similarly, unsecured access by third parties also has been the source of data security glitches. In a recent data breach affecting sandwich maker Jimmy John's Franchise, LLC, hackers purportedly compromised consumer credit and debit card data between June and September at some of Jimmy John's company-owned stores and franchised locations.[9] According to Jimmy John's, its investigation determined that an "intruder" was able to remotely access point-of-sale systems by using stolen third-party log-in credentials from one of Jimmy John's point-of-sale vendors.[10] Likewise, International DairyQueen, Inc. suffered a data breach related to its insiders.[11] In October, hackers reportedly installed malware on DairyQueen systems by using "compromised account credentials" from a third-party vendor.[12]

A third-party weakness in the insider chain also served as the focal point of a data breach at Goodwill Industries International, Inc. Goodwill announced that between February 10, 2013 and August 14, 2014, malware installed a third-party vendor's systems compromised certain of its customers' payment card information.[13] Although Goodwill determined that there was no malware installed on any of its internal systems, the attack nevertheless impacted 20 of its members, or about 10% of all of its stores, that used the same third-party credit card processor on which the malware was installed.[14]

Financial institutions risk unauthorized access to their systems as a result of weak insider behavior as well. In early October, JPMorgan Chase & Co. notified the Securities and Exchange Commission (SEC) that it believed a data breach impacted 76 million households and seven million small businesses in June and July of this year, which compromised its "user contact information."[15] Hackers apparently accessed the bank's computer systems and servers after having obtained a list of applications and programs that ran on the bank's computers and used it to access the bank's systems through a vulnerable entry point.[16] Here, an employee's personal laptop reportedly served as the access point on which the hackers installed malicious software that allowed access into JPMorgan's network.[17]

How Can the NIST Framework be Applied to Insider Threats?

In February, the National Institute of Standards and Technology (NIST) released its inaugural *Framework for Improving Critical Infrastructure Cybersecurity* (Framework).[18] As its name suggests, the Framework focuses specifically on cybersecurity related to "critical infrastructure." The executive order that mandated the creation of the Framework defines "critical infrastructure" as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[19] While many organizations or functions within the FinTech community do not fall within this narrow definition of "critical infrastructure", the Framework still provides a helpful reference for addressing cybersecurity risks. Specifically, the Framework's risk management approach and example controls can be used to evaluate and counteract the cyber threats caused by insiders.

Risk Management

The voluntary Framework sets forth a flexible risk management methodology that can be used to evaluate the risks associated with cyber threats that are faced by FinTech organizations of varying sizes, risk profiles and complexities.[20] The Framework's approach is to identify those cyber threats that are applicable to the organization, assess the likelihood that each event will occur and the resulting harm, and then address those cyber threats based on the organization's self-selected risk tolerance. This approach is very likely similar to, if not the same as, the risk management methods that risk managers within FinTech organizations already use to assess financial, operational and other types of risks facing their organizations.

The Framework recognizes that cyber risk factors, including those associated with the cyber threats caused by non-malicious insiders, are unique to a particular organization and cannot be determined in a one-size-fits-all approach.[21] This flexible approach allows FinTech organizations to address and respond to cyber risks in different ways that are compatible with their different sizes, complexities, resources, and risk tolerances. With respect to the insider threat, the uniqueness is caused in part because FinTech organizations have different types and numbers of employees, utilize contractors in different ways to fill various internal functions, and have varied supply chains that collectively create a risk profile that is unique to each organization.

The first step in conducting the risk assessment is to identify those cyber threats that are pertinent to the organization. When applied to the insider threat, each organization has to first discover and then catalog those insider threats that are relevant to them. This discovery process usually starts with evaluating the number, type and location of all insiders—both internal employees and external contractors. It is important to understand how these insiders interact with the organization's systems and data. For example, can they install unapproved software on their organization-issued computers or connect to the network using their personal devices? Within many organizations a natural insider hierarchy will be present. There will be a small number of insiders at the top of the pyramid that have privileged access to mission critical systems and the organization's most sensitive data. These trusted insiders, like system administrators and senior management, also are the most likely to have the most flexibility to circumvent security controls and often are subject to the least routine security monitoring. Given the different degrees of access, different types of insiders will present different types of risks. Since "insiders" also include individuals outside an organization, ways in which vendors and suppliers could negatively impact system security should be considered. For example, it is unlikely that prior to the breach of the vendor that processed credit card information for certain Goodwill members, Goodwill would have anticipated that the source vulnerability would have been caused by malware on its third-party vendor's systems.

Then, once that assessment is done and based on this risk profile, the organization needs to determine the probability that any one of these insider risks will arise and, if it arises, what kind and amount of harm it will cause. Past incidents within an organization and within a sector are good indicators of the likelihood that a particular threat will present itself. Other types of common threats—lost devices, phishing emails, written-down password—are all almost guaranteed to happen in any sizeable organization. With respects to quantifying the harm, remember, that it should not be limited to financial harm. Consideration also should be paid to the operational impact, damage to reputation, loss of good will, and other forms of qualitative harm. In addition, security incidents also increase the occurrence of litigation, government action, negative media coverage, or other damaging events beyond direct financial harm. All of these adverse impacts of a potential security incident need to be considered in the risk analysis.

Finally, many organizations will then rank in order the various risks that they face based on the product of this probability score and the estimated harm level. Those incidents that are the most likely to occur and that could cause the most amount of harm rise to the top of the ranked list. A very harmful incident that is not likely to occur might be ranked below less harmful incidents that occur more frequently. This ranking can be helpful in comparing threats with varying degrees of likelihood and harm, and also for prioritizing those threats that, assuming limited resources, should be addressed first. There is one type of exception that should be noted: black swans.[22] There are some highly improbable security incidents that obtain a higher prioritization and get addressed even though they are very unlikely to occur because they could cause extremely negative impacts on an organization.

Finally, once the organization conducts a risk assessment, it can perform a gap assessment to determine whether they have sufficient administrative, technical and physical controls in place that effectively compensation for the identified risks.

Framework's Example Controls

The Framework also provides an example set of controls that can be used to address cyber threats from insiders. These controls are organized into five functional groups: identify, protect, detect, respond and recover.[23] The administrative, physical and technical controls provided within the

Framework are not exhaustive or exclusive; they cannot be applied blindly, but are a helpful starting place for organizations that do not otherwise already have a security program that addresses insider cyber threats.[24] Within each function group, there are several categories of controls that are especially relevant to addressing the inadvertent or unintentional cyber threats caused by insiders.

Business Environment

One of the most important activities an organization can perform is to thoroughly understand the contours of its environment.[25] Where the data is stored, what systems and applications are being used, and how individuals within and outside of the organization are interacting with systems and data. A common exercise is to map the flow of data through the point in time it is collected, where it is processed and stored, when and how it leaves the organization, and how it is securely destroyed. If an organization does not know what data it has and how that data is being used, then the organization cannot apply the appropriate security controls or, potentially, even know when a system has been compromised or data has been breached or removed.

For many organizations, their use of contractors and vendors also has a significant impact on their security posture. Just like an organization must understand its own systems, an organization also must understand the dependencies and contingencies created by external parties that connect into its systems or that supply its hardware or software. As demonstrated by the recent credit card breaches at Goodwill and DairyQueen, cyber attackers will look for and exploit an organization's weakest link, including those outside of it. Knowing and understanding the larger picture will allow security teams to implement those precautions that are appropriate across an organization's entire environment.

Awareness and Training

The cliché is true, knowledge is power. Most insiders are well-intentioned and do not purposefully try to create security vulnerabilities for their organizations. However, if insiders do not understand what security threats can be avoided and how to utilize the security tools that exist within their organization, they will not be in a position to help their organization avoid or mitigate security threats.

The Framework's example controls make clear that *all* insiders need to be trained.[26] Importantly, this includes executives and outside vendors.[27] Attackers frequently target executives with spear-phishing emails and other directed tactics because the attackers know that these insiders are often given broad (and unnecessary) access to many systems by default, frequently have very poor security hygiene and, unlike other lower-level employees, are not always subject to the same level of network surveillance or security controls.[28] Just like internal employees, contractors and vendors also need adequate security training and awareness.[29] To minimize the risk of co-employment issues, organizations often require vendors to represent that their security training satisfies a minimum standard or, alternatively, to deliver training to their own employees based on content developed by the organization.

The fact that all insiders need to be trained does not mean that they should all be trained on the same content or in the same way. Training should be based on the insiders' roles and responsibilities; for example, general security training should be different from the training provided to security personnel. Raising the security awareness of insiders is probably the quickest and most cost-effective way to increase an organization's security posture. The following section provides some recommendations on how security training can be more effectively provided to all of an organization's insiders.

Access Controls

One of the most common insider caused vulnerabilities that results in the loss of data is when the attacker takes advantage of network access rights granted to a legitimate user.[30] For example, compromising an administrator's network username and password, which already has the ability to access many different systems, or exploiting the organization's internal identity management systems to elevate the privileges of a lower-level employee's network username and password that have been compromised. An organization makes this type of attack even easier when it has not appropriately limited a user's access level based on the user's function and role within the organization and, thus, has given the user broad access by default. Once this type of username is compromised the attackers have immediate access to a wide range of systems.

The Framework provides example controls that address multiple aspects of network access. First, it includes example controls that recommend that local and remote access be actively managed by the organization and not set by default.[31] While organizations frequently pattern a new user's access rights based on an existing user, this can set a dangerous pattern of giving users access to systems based on convenience and not based on need. The example controls also recommend that organizations consider separating duties and segregating system access.[32] Like the launch keys on nuclear submarines, it is increasingly common to require two independent passwords from different administrators before restricted systems can be used to take especially sensitive actions, like exporting large amounts of data or adding other administrative users. This helps to reduce risk because both of the separate passwords would have to be compromised before the attacker could take the action. Within a FinTech organization, this heightened level of access control may be appropriate for the encryption key management system or tokenization system that, if accessed, would allow an attacker to access the organization's most sensitive systems or data. This is not without costs; this type of dual key system adds complexity and additional time to any process that is dependent on getting both individuals to initiate the action.

Many organizations are also implementing physical and logical segmentation to those systems that have the highest risk, like those systems that maintain credit card data. Some FinTech organizations are building separate and discrete networks to make it more difficult for attackers to get access to these highly-restricted systems via compromising another part of the internal network. For instance, network segmentation is a recommended, but not a required, method to limit the scope of the Payment Card Industry Data Security Standard.[33] Many organizations are using segmentation to de-scope parts of their network and lower their compliance burden. However, a drawback to segmentation is that it can be very expensive to implement and it can cause additional operational complexities for systems and applications that were originally implemented on a flat network.

Lastly, the Framework recommends that an organization grant the lowest level of access by default and higher access only by exception after review and approval.[34] This "least privileges" approach is a common starting point because a user's internal access rights will often naturally increase over time. Access rights need to be reviewed periodically to ensure that the rights are still appropriate for the insider's position within the organization. This review is especially important and often overlooked when an individual changes roles within an organization.

Data Security

The Framework, like many other security standards, puts a good deal of emphasis on applying security controls to the data itself so that the data is protected in storage and transit. The Framework avoids recommending or referencing any particular type of technology, but data security techniques like hashing, encryption and tokenization are being used by many FinTech organizations. These techniques help protect sensitive data, like payment information and passwords, while they are stored in or processed by internal systems.

The Framework recommends that organizations have formalized processes and procedures that address the removal, transfer and destruction of data.[35] These points of transition—like when data is being moved between systems or when it is scheduled to be destroyed—are when the data is the most susceptible to compromise. This is because the data is commonly unshackled from the protections that were applied when the data was at-rest so that it can be processed or inspected. While many organizations readily see the need to protect the transmission of data when it leaves the boundaries of their network, more and more organizations also examining how to protect internal-to-internal data transmissions to limit an attacker's ability to access the data from other unrelated internal systems. In addition to protecting the data directly, organizations frequently implement data loss-prevention tools to monitor the movement of data and proactively attempt to stop the transfer of certain sensitive data elements (*e.g.*, Social Security numbers, driver's license numbers, or payment card information) before they leave the network.

Data security is particularly helpful because even when attackers gain access to a network or systems, if the data itself is protected it may be of no or limited value.

What is the Role of Counsel in Helping Address the Insider Threat?

Today's cyberattacks come from a variety of directions. Even those that originate outside of an organization often leverage a vulnerability caused by a legitimate user inside of, or connected to the organization's network. Organizations that work to increase their understanding of how their own insiders can impact their overall cyber exposure can use this understanding to significantly improve their overall security posture. In-house counsel have certain knowledge, skills and experience that can be used to help their organizations address this insider threat.

The following outlines three core recommendations that organizations can use to better address the non-malicious insider threat. First, apply enterprise risk management programs to cybersecurity risks, including those risks created by insiders. Next, increase the frequency and relevancy of security training. Make sure that everyone has training designed to raise their awareness of those security threats that they are likely to face in their role. Lastly, the security tools used by an organization to protect its data and systems must be "easy" for the average insider to use. Security tools that get in the way of productivity or impede legitimate business activities will eventually be bypassed. Security needs to be incorporated into the day-to-day operations so that security is in place by default and not by happenstance.

Risk Management

As discussed above, organizations need to apply their formal risk-management processes to cybersecurity. This risk examination cannot focus solely on external factors but must also include those threats from within. The training and experience of attorneys makes them a specialized form of risk manager. They often have experience in helping their clients understand, predict and quantify legal risks. Counsel can utilize this experience to help assess different cybersecurity risks associated with their organization's insiders.

An organization's attorneys should volunteer to participate with their business peers in the periodic cyber-risk assessment sessions. In addition to their experience as risk evaluators, attorneys may also have firsthand knowledge of particular insider problems that are already plaguing the organization. This is important because the list of relevant threats should include those incidents that are already occurring within the organization or within its sector. In addition, the risk assessment should also look at insider threats that are common to all organizations, or relevant to unrelated entities outside their sector but that utilize a common infrastructure or systems.

However, some attorneys have a reputation for being too risk-averse, which could impede rather than enhance data security efforts. Thus, counsel should keep two ideas in mind to optimize their participation in the risk-assessment sessions. First, the primary objective in any risk-management exercise is to prioritize risk and not eliminate it, an impracticable and impossible task. This prioritization will help an organization to determine which risks should be addressed first, which can be deferred until later, and which can just be assumed by the organization and not addressed at all. This is especially important because most organizations do not have an unlimited amount of resources—financial, time or human—to try to tackle every possible risk. Those risks that are unlikely to happen, are adequately contained by existing mitigation efforts, or that only result in a negligible amount of harm can be de-prioritized. Some attorneys will have to adjust their own personal risk aversion and get comfortable with the fact that some risks will be left unaddressed.

Second, threats should not be viewed through a *worst-case scenario* prism. Not all risks will cause cataclysmic damages to, or bring about the end of the organization. Cybersecurity risks should be kept in perspective and normalized for other comparable risks, and the ultimate risk level may be lowered with the use of effective compensating controls. Counsel may need to rein in their *sky is falling* mentality in order to keep these risks in perspective.

Counsel may take the same types of skills that they already use to evaluate litigation, regulatory and other legal risks and apply those to assessing this type of cyber risk. So long as counsel can remember the objective of the risk assessment and can check any personal tendencies to be too risk-averse, they can be a valuable part of the team and help their organizations become more risk-aware.

Training and Awareness

Insider education and awareness is one of the most important and cost-effective approaches that any organization can take to increase their security. Given the unavoidable "human factor," an organization's security teams will have to work hard in order to make the security controls as easy and as transparent as possible for insiders. Insiders serve on the front lines of the security defenses and, without proper training, they will open the doors and let the attackers in. Yet, with proper training, they can add another critical layer of defense that may be able to stop the attack or ring the alarm when they witness suspicious activity. In order for insider training to be effective, it must be relevant and timely, must include all of the insiders, must address personal devices and social media, and must allow insiders to sound the alarm when they observe security anomalies.

Security training should be appropriate and germane to the insider's role in its organization. It is no longer sufficient to sit everyone down on their first week and have them listen to the security training video or "sign off" on the security manual, which may or may not have been updated in a couple of years. There must be baseline security training on topics that are applicable to all insiders, such as secure password practices, email safety, connecting to the corporate network from home, reporting security violations, etc. Then, additional security training may be customized so that it relates to those specific threats that each audience of insiders is likely to face. For instance, employees in a call center need to know more about social engineering and how to properly store sensitive customer information in the designated fields of customer databases. Meanwhile, application developers may need specialized training on secure coding practices because that is relevant to their role. This tailored training may be grouped for insiders with similar roles.

Organizations are also experimenting with just-in-time and contextualized learning. This is training that is delivered right before the content is needed and in context with the user's actions.[36] For example, if an insider was reviewing instructions on how to use the organization's email program, the instructions would also provide contextual security training on why not to open attachments from unrecognized senders and how to report emails that appear to be phishing for information.[37] Similarly, some organizations are starting to introduce training content outside of their formal training systems, like security newsletters, security awareness activities, and short 30-second security "commercials" that play when a user first logs into their computer. Training offered once a year or just at the time of hire is not enough; in order to raise security awareness organizations must find dynamic ways of regularly introducing security training amongst their insiders.

The training should be short. Research conducted on the edX's open online course library suggests that the optimal length of video-based training should be six minutes or less, otherwise trainee engagement starts to drop.[38] At this short length, security topics need to be broken up so that they can more easily be segmented into short training modules. Shortened training courses also benefit the organization because they are easier to schedule and are less disruptive to business operations since they do not require insiders to be away from their work for long periods of time. Also, shorter training sessions can be given more frequently throughout the year without being more of a burden.

The more rights and access that insiders have within an organization means that they will need more training and a higher degree of security awareness. A group that commonly gets bypassed by the required training is the organization's senior managers. Often they are "too busy" or no one wants to bother them to make sure that they have taken the required security training. This is especially dangerous for this group because they are frequently targeted by attackers as they often travel outside the office necessitating that they connect to untrusted networks that are more difficult to secure, often use the newest devices that have not been fully vetted, and are also more prone to lose their phones or laptops. These individuals also routinely have default access to a broad set of systems and data, which means when their accounts or devices are compromised, the attackers are able to obtain a wealth of information directly or have the *de facto* means to access other internal systems. Organizations will have to find innovative ways to raise the security awareness of their senior managers.

Training today is not limited just to organization-issued devices and internal systems. Even when an organization has not adopted a "bring your own device" policy, more and more insiders are using their personal devices to conduct business by accessing their work email on personal smartphones or connecting back into the corporate network from their home PC. The recent data breach at JPMorgan that affected more than 70 million households reportedly originated when attackers were able to install malicious code on a bank employee's personal computer and then utilized that compromised personal device to move further into the bank's internal systems.[39] Any device that connects to or communicates with an organization's internal systems has the potential to be a way in to steal its data. Thus, effective training needs to address when and how individuals may use their personal devices for work and, when permitted, what steps must be taken to help protect the systems and data while they are connected to the network.

Training, however, cannot be limited to personal devices. More and more people are using social media for both personal and professional reasons. Training should caution insiders about sharing information online that could compromise an institution's security. For example, "out-of-office" email notifications illustrate a potential weakness. If an employee's title is "senior database administrator" and that employee broadcasts to the world that she will be away on vacation in a region where she will not be checking her work email, she may just be signaling to a prospective attacker that they should try to change her network password through social engineering during a time when she is less likely to notice any changes to her password. Lastly, social media may be a threat itself since there have been reports that some cyber criminals may be posing as recruiters in order to identify and compromise an organization's insiders.[40]

Finally, insiders have to be able to sound the alarm. Training and security awareness materials that provide clear directions on when and how to report suspected security breaches serve to boost data security efforts. An organization cannot take advantage of the thousands of ears and eyes associated with its insiders unless it has a systematic way to funnel their reports to its security teams. Easy to use email addresses or telephone hotlines are one way to encourage insiders to report potential security more quickly. When reported, an organization must have the teams and response plans in place and be ready to respond. There is nothing worse than when someone promptly alerts an organization to a security problem only for it to remain unread or not responded to because the organization failed to appropriately staff or prepare its security teams.

An organization should also consider how its external contractors and vendors may report suspected security problems. If they are not able to access the same mechanism used by its employees, the organization should consider establishing clear points of contact that can be provided during the vendor on-boarding process. Relying on vendors to contact their business point of contact with security concerns may take too long and be a less reliable way to get this information into the hands of the teams that are prepared to respond.

Counsel can help in two ways. First, they must take the security training and awareness courses. Counsel often have access to the most sensitive and proprietary information within an organization. Being trained will help ensure that they are properly protecting this information when it is saved or shared in and outside of the organization. Being properly educated about how to use the security tools available within the organization should also help its attorneys from inadvertently creating security problems. Secondly, inside counsel must be a cheerleader for good security practices. As they work with internal clients, they should set a good example of how to follow the organization's security protocols. When their internal clients or legal colleagues need security assistance, they should direct them to the training and awareness materials that are available. Even better, they can connect them with someone in the security department that can help apply the appropriate security controls to their business project. If counsel assist with contract negotiations, they should make sure the vendors have been run through the organization's security due diligence process so that any security considerations can be included in the contract.

A properly administered security training and awareness program can be a cost-effective way to increase the security of an organization. In order to leverage an organization's insiders to assist in its defense, it must equip them with the knowledge about how to use the existing security tools that are available and how to promptly report security issues to the organization's team of security first-responders.

Security Must Be Easy and by Default

The reality (and challenge) is that security is inconvenient. It takes longer, it is harder, and often gets in the way of whatever the organization's insiders are trying to accomplish. To be effective, security needs to be *easy*. In order to be easy it needs to be automatic. It needs to be running in the background and as transparent as possible to the insiders. Automated security controls—like end-to-end encryption and data loss prevention systems—that can be running without any action or intervention from insiders are more likely to be effective. They are more effective because they are less likely to get in the way of business activities, and then get turned off or circumvented by insiders. In addition to being automatic, security also needs to be the default in as many areas as possible. Insiders are creatures of habit; they are not likely to turn security on without prompting, but they are also not likely to turn security features off unless they are given a reason.

An insider already has too many passwords. The average person is trying to remember the passwords for 25 personal and professional accounts at any given time.[41] To make matters worse, it is common to have different password complexity requirements—minimum number of characters, use of uppercase and lowercase values, mix of numbers, letters and special characters—that makes it more difficult for someone to remember *all* of their passwords. As a result insiders are doing one of two things. They are writing down their passwords—on sticky notes under their keyboard, in notes on their phone or, even worst, in files kept by their administrative assistant. Or, they have adopted a scheme to make the password easier to remember which in turn usually makes the password easier to guess. FinTech organizations can help by consolidating the number of passwords that are needed within the organization. This frequently is facilitated by a single-sign-on system that allows insiders to use a single username and password to login to all or many of the standalone systems that formerly required a unique username or password. Reducing the number of passwords will increase the security of the organization because fewer passwords will be lost or compromised as a result of poor password habits.

FinTech organizations can also help by evaluating new methods of allowing users to create passwords that are both difficult to crack and also easier to remember (without the sticky notes). Early research out of Carnegie Mellon University's CyLab suggests that it is actually more secure to allow the use of passphrases instead of complex passwords.[42] A passphrase is a string of common words that are otherwise unconnected and have no meaning on their own. For instance, a passphrase could be a color, animal, thing and place—"OrangeGoatBusNewYork." The passphrase ends up being longer than the average 8-to-10 character passwords and because it can be expressed in a standard sentence ("I saw an *orange goat* driving a tour *bus* in *New York*") passphrases are easier to remember. A passphrase like the above has 93.1 bits of entropy which would take billions of years longer to crack then a standard 8-to-10 character password.[43]

Another principle of human nature to keep in mind is that people cheat. When things become too difficult, when they run out of time, or when security becomes an impediment to accomplishing a business priority, even well-intentioned insiders will cheat. Cheating is usually a signal that security programs are causing friction within the organization. To help reduce this friction, stringent security controls should only be applied on an *as needed* basis because applying them too broadly will encourage more cheating. Additionally, many security controls are launched with very little or no user testing. The result is that the controls work well in theory but not in practice. They do not interoperate well with other internal systems, are not intuitive enough for insiders to understand how to use without more in-depth training, or do not mesh well with the culture of an organization. Security departments should conduct extensive user-acceptance testing, solicit and incorporate feedback and rigorously test the new insider-facing security systems before they are deployed into production. This up-front work will help to minimize the number of insiders that fail to utilize the security controls or, because they interfere with existing business practices, try to circumvent the organization's controls.

When insiders violate the organization's security rules there must be enforcement with meaningful consequences. Rules that are not actively enforced are not effective. A lack of consequences within an organization suggests that security is not a valued priority. Enforcing an organization's security rules demonstrates that security is a priority and an important value to the organization. Adequate enforcement also helps create a culture of personal responsibility that reinforces that all insiders, at all levels, have an important role in helping protect the organization's electronic assets. Building this culture has to start at the top, if an organization's senior managers openly boast about not following the internal security protocols or ignoring security standards when implementing business projects, then their teams will get the message that security is not important, it is not a priority, and can be openly circumvented without consequence.

As noted above, cheating is usually a symptom that one of the controls is causing friction within an organization. There are several common things that might be causing this friction. First, the security controls are overly restrictive. Organizations should apply the most onerous security controls *only* to their most sensitive systems and data. If they try to apply those same heightened controls everywhere and to everything, then they are not recognizing that there are varying degrees of security and not everything needs maximum protection. An organization's security programs need to be balanced and reasonable, given the associated riskiness of the situation. Second, the friction may be a signal that the security control is not well-implemented from within the organization. If the control does not work well with other internal systems or interferes with legitimate business practices, insiders will always choose business priorities over security considerations. This underscores the importance of conducting an impact assessment and user-acceptance testing; indeed, the organization should treat the roll-out of new security controls much like it would roll out any new consumer product to help ensure that the control can and will be adopted. Last, failure to adopt may result because insiders do not know how to adopt the control, or do not understand the importance of the control. An organization can minimize this point of friction with a good security training and awareness program.

Conclusion

FinTech organizations are under a constant and growing cyber assaults from attackers that want to disrupt their systems and steal their data. In addition to traditional hardware- and software-based security controls, FinTech organizations should evaluate and address those cyber risks caused by its insiders—both within and outside of their organization. These insiders have been the root cause of recent cyber events and organizations can increase their security posture by increasing their focus on addressing these insider threats.

Nevertheless, organizations that can incorporate the insider threat into their risk assessment, increase their focus on security training and awareness, and work to make their security controls easier and more transparent will improve their ability to identify, respond to and recover from cyber threats caused by insiders.

NOTES

[1] The Cybersecurity Framework, launched in February, was compiled by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) with input from the private sector. The Framework represents efforts to develop a voluntary how-to guide for key organizations with critical infrastructure to enhance their cybersecurity. The Framework is a key part of Pres. Obama's Executive Order on "Improving Critical Infrastructure Cybersecurity" that he announced in the 2013 State of the Union.

[2] Wade H. Baker et al., Verizon Business, 2014 Data Breach Investigations Report (DBIR) at p. 6 Fig. 2 (Apr. 2014), *available at* http://www.verizonenterprise.com/DBIR/2014.

[3] *2014 Cost of Data Breach Study: United States*, conducted by Ponemon Institute and sponsored by IBM (May 2014), *available at* http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/ (registration required).

[4] *See e.g.*, Prepared Statement of the FTC, *Data Breach on the Rise: Protecting Personal Information from Harm* before the Committee on Homeland Security and Governmental Affairs, U.S. Senate (Apr. 2, 2014); *see also* Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8616, 8633 (Feb. 1, 2001) (Intending to protect customer information held by banks and requiring regulated banks to "implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities.")

[5] Prepared Statement of the FTC, Data Breach on the Rise, *supra*.

[6] *In Re TJX Cos., Inc.*, No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter.

[7] Nathalie Grover and Narottam Medhora, *AT&T says some customers being informed of August data breach*, Reuters.com (Oct. 7, 2014), *available at* http://www.reuters.com/article/2014/10/07/us-at-t-cybersecurity-idUSKCN0HW02Y20141007.

[8] Vermont Department of Consumer Protection, Data Security Breach Notice Letters, AT&T letter to Consumers re. Security Breach (Oct. 1, 2014) (disclosing employee accessed account information without authorization), *available at* http://ago.vermont.gov/assets/files/Consumer/Security_Breach/AT&T%20ltrt%20Consumer%20re%20Security%20Breach.pdf.

[9] Press release, Jimmy John's Franchise, LLC, "Jimmy John's Notifies Customers of Payment Card Security Incident" (Sept. 24, 2014), *available at* https://www.jimmyjohns.com/datasecurityincident.

[10] *Id.*

[11] Announcement from Pres. and CEO John Gainor, Am. DairyQueen Corp., Data Security Incident, (Oct. 9, 2014), *available at* http://www.dairyqueen.com/us-en/datasecurityincident/?localechange=1&.

[12] *Id.*

[13] Press release, Goodwill Industries International, "Goodwill Provides Update on Data Security Issue" (Sept. 2, 2014), *available at* http://www.goodwill.org/press-releases/goodwill-provides-update-on-data-security-issue.

[14] *Id.*

[15] JPMorgan Chase & Co., Current Report (Form 8-K), (Oct. 2, 2014), *available at* http://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm.

[16] Jessica Silver-Greenberg et al., "JPMorgan Chase Hacking Affects 76 Million Households,", New York Times (Oct. 2, 2014), *available at* http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0.

[17] Emily Grazer and Danny Yadron, "J.P. Morgan Says About 76 Million Households Affected by Cyber Breach," Wall Street Journal (Oct. 2, 2014), *available at* http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

[18] Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, The National Institute of Technology & Standards (NIST) (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[19] Exec. Order No. 13636, 78 Fed. Reg. 33 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

20. Framework, *supra* at 5.
21. *Id.* at 7 §1.2.
22. Nassim Nicholas Taleb, The Black Swan: The Impact of the Highly Improbably (2010 Random House Trade Paperbacks, 2nd ed. 2007).
23. Framework, *supra* at 7, §2.1.
24. *Id.* at 20, Appx. A, Table 2.
25. *Id.* at 21, Appx. A, Table 2, Business Environment.
26. *Id.* at 24, Appx. A, Table 2, Control PR.AT-1.
27. *Id.* at 24-25, Appx. A, Table 2, Controls PR.AT-3, PR.AT-4.
28. "Spear phishing" is a phishing attack, see note 41, that is directed at a specific individual or company.
29. *Id.* at 24, Appx. A, Table 2, Control PR.AT-3.
30. Verizon DBIR , *supra* at p. 6, Fig. 2.
31. Framework, *supra* at 23-24, Apps. A, Table 2, Controls PR.AC-1 and PR.AC-3.
32. *Id.* at 24, Appx. A, Table 2, Controls PR.AC-4 and PR.AC-5.
33. Payment Card Industry (PCI) Data Security Standard, Version 3.0, Payment Card Industry Security Standards Council, p. 11 (Nov. 2013).
34. Framework, *supra* at 24, Appx. A, Table 2, Control PR.AC-4.
35. *Id.* at 25, Appx. A, Table 2, Control PR.DS-3.
36. Margery Weinstein, "Just-In-Time Technology Solutions," Training Magazine (Sept. 29, 2014), *available at* http://www.trainingmag.com/trgmag-article/just-time-technology-solutions.
37. "Phishing" is the practice of sending emails that look like they originate for a legitimate sender but are actually from a third party that is trying to get the recipient to respond with their information, like their password or Social Security number, or to click on an embedded link that will install malware.
38. Philip J. Guo et al., "How Video Production Affects Student Engagement: An Empirical Study of MOOC Videos,"Association for Computing Machinery, Conference on Learning at Scale (Mar. 2014), *available at* http://pgbovine.net/publications/edX-MOOC-video-production-and-engagement_LAS-2014.pdf.
39. J.P. Morgan Says, *supra*.
40. Robertson, Jordan, "Does that headhunter want your head, or your secrets?," Bloomberg (Sept. 16, 2014), *available at* http://www.bloomberg.com/news/2014-09-16/does-that-headhunter-want-your-head-or-your-secrets-.html.
41. Dinei Florencio & Cormac Herley, "A Large-Scale Study of Web Password Habits," International World Wide Web Committee (May 8-12, 2007), *available at* http://research.microsoft.com/en-us/um/people/cormac/Papers/www2007.pdf.
42. Richard Shay et al., "Can Long Passwords Be Secure and Usable?," Special Interest Group on Computer-Human Interaction, Conference SIGCHI 2014 (Apr. 26 – May 1, 2014), *available at* http://www.blaseur.com/papers/chi2014-long-passwords.pdf.
43. *See*, Tyler Akins, *Strength Test*, http://rumkin.com/tools/password/passchk.php (last visited Oct. 24, 2014); and *How Secure is my Password?*, Sponsored by RoboForm Password Manager, https://howsecureismypassword.net (last visited Oct. 24, 2014).