The International Family Offices Journal

Contents

Volume 1, Issue 1, September 2016

1 The characterisation of the dominant ethnic cultures in the world as being 'Western individualistic', 'collective harmony' or 'honour' is taken from the 2016 book entitled *Cross Cultures; How Global Families Negotiate Change Across Generations*, by Dennis T Jaffe and James Grubman.
2 INSEAD Professor Randel Carlock has written of how many Asian families have an espoused value of family harmony – yet it is often not an enacted value, and hence the prevalence of family feuds in Asia despite the cultural importance, in theory, of preserving family harmony. See "Solutions for infighting among Asian business families", Randel Carlock and Loh Keng Fun, *South China Morning Post*, 5 June 2015.
3 John Davis, *Next Generation Success* (Cambridge Family Enterprise Press, 2014).
4 Randel Carlock and John Ward, *When Family Businesses Are Best* (Palgrave Macmillan, 2010).
5 Ivan Lansberg, *Succeeding Generations* (Harvard Business Press, 1999).
6 Ken McCracken, "STEP Advanced Certificate in Family Business Advising" (course brochure).
7 Carlock and Ward, note 4 above.
8 Carlock and Ward, note 4 above.
9 Lansberg, note 5 above.
10 DT Jaffe, *Stewardship in Your Family Enterprise* (2014).
11 Jaffe, note 10 above.
12 Jaffe, note 10 above.
13 Palgrave Macmillan, 2010.
14 Ward, "The ultimate vision for continuity?", *Families in Business*, Sept/Oct 2003.
15 Harvard Business School Press, 1999.
16 Jaffe also writes: "Each generation of the family must get together and ask, 'What is our purpose relative to the business and to each other?'" – see *Stewardship in Your Family Enterprise* (2014).
17 "The Dreams that Drive Business Success", *Families in Business Magazine*, Spring 1999.
18 Professor Roger King, Hong Kong University of Science and Technology.
19 See www.thewesleygroup.com/blog/?p=348, posted 21 March 2013.
20 Mesatop Press, 2009.
21 Hauser's comments are from a Family Office Association Q&A paper entitled "When Mission Statements do more than collect dust".
22 Wiley, 2nd edn, 2004.
23 Hughes' comments are also drawn from the Family Office Association Q&A Paper "When Mission Statements do more than collect dust".
24 Bloomberg Press, Wiley, 2007.
25 Wiley, 2014.
26 See Family Office Association Q&A Paper "When Mission Statements do more than collect dust".
27 Professor Roger King, Hong Kong University of Science and Technology.
28 Unfortunately for the members of the rising generation of the family, if these paper exercises have been incorporated into the terms of family trust structures, perhaps through the letter of wishes, there can be non-family trustees and advisers who may be very happy to enforce their terms literally on the family.
29 See footnote 4 above.
30 A primary focus of *Cross Cultures* is on how to help the members of the rising generation of a family from a collective harmony or an honour culture, who have been exposed to Western individualistic culture, negotiate across cultures with their elders.
31 Hartley Goldstone of Wise Counsel Research Associates stresses this last point and points to the book *Rethinking Positive Thinking* by Gabriele Oettingen (Penguin Random House, 2015).

Cybersecurity and the family office

Holly Isdale

Mention IT and data security in any conversation and most people's eyes glaze over. Like dietary fibre or exercise, cybersecurity is one of those things that you know is good for you but rarely seems tasty or interesting in large doses. Yet, on any day, in any major newspaper or newsfeed, you are guaranteed to find an article that touches on a security breach at a large institution or an act of cyberterrorism somewhere in the world. Cybercrime is now big business and, day by day, the cost of entry is getting lower and the payoff higher for professional cybercriminals. Families and family offices need to refocus their attention on this area, which is expected to be the single most important area of risk management for the coming decades.

Cyber security, and information security generally, were generally put on the back burner as a topic of risk management until perhaps 2012 or 2013, at which point cloud computing, and the security issues it presented, became harder to ignore. In 2013, the breach of Target stores in the United States, and the subsequent release of the consumer records of 70 million customers, showcased the vulnerability of large, well-funded programmes when those programmes' partners had weaker security processes in place. Further, enactment of the Health Insurance Portability and Accountability Act in the United States dramatically spread the liability, accountability and consequences of privacy issues

IT security began to emerge as a hot topic for conversations, and attracted talent on both sides of the legitimacy spectrum. In the following year, the world experienced a spike in data breaches, which expanded from one-off or loose affiliations of hackers to organised efforts to target large companies or financial institutions. By late 2014, we saw a hack of Sony Pictures Entertainment, which later was alleged to have been sponsored by North Korea, a unique but not unprecedented attack on a private company by a sovereign nation.[1] In 2015, the number of high-profile attacks continued, from the US Office of Personnel Management,[2] US health insurance firms Anthem[3] and Premera,[4] to hotels (Hilton,[5] Mandarin Oriental,[6] and even Trump Hotels[7]), to the sex industry (Ashley Madison[8]) and even toymakers (V-Tech[9]). In fact, the number of reported cyber breaches surged by 38% in 2015 over the comparable 2014 statistics and were estimated to cost affected businesses between US$300 billion and US$1 trillion annually.

Yet most breaches go unreported, in part owing to the damage to reputation and potential liability if breaches are disclosed by the affected party to its customers, to other vendors or to government authorities.[10] Globally, it is estimated that IT security will have consumed more than US$100 billion in investment by 2018 and the cybersecurity market in the United States alone is expected to be US$170 billion by 2020.[11] Cyber insurance, a novelty product just a few years ago, is expected to reach US$7.5 billion in premiums by 2020 (up from US$2.5 billion in 2015).[12]

Despite these alarming statistics and headlines, most wealthy families and family offices are woefully unprepared to assess their risk of loss or to take action in the event of a breach. Family offices have a unique, and rather complicated, cyber footprint. The office exists to serve the family and there is a responsibility to identify (and mitigate) risks to the family. But how the family itself manages its data and cybersecurity needs, while critical, is often beyond the immediate control of the family office.

The family office must manage the flow of information into the office and out to its partners, communicating sensitive information up to the family in an orderly and secure manner, ensure secure communication to advisers (attorneys, accountants, consultants and others) that will not void various legal privileges protecting the discussions, and then manage the daily communication down to investment managers or asset/entity operations. These data feeds are often outside the control of the family office and yet present vulnerable entry points for data breaches. In addition, of course, the family office is a business unto itself and needs to manage its employees and independent contractors in terms of how they handle and transmit data or use computer systems. The family office should have a cyber policy in place to safeguard data and establish procedures for its own operations.

So how can we protect our families and our family office information from the increasing threat of breach? First and foremost, all families and family office professionals need to get educated about the nature and extent of the risks they face. Secondly, families and family offices need to develop robust plans to manage the risk and to operate in the event of a breach, either of their own systems or of the data that is held by an outside vendor or third party. Finally, as painful as it may be, the family office needs to be able to require all employees and family members, as well as outside advisers or consultants, to adhere to whatever risk protocols the family office has identified as necessary in order to minimise the occurrence or extent of a security breach. Each of these aspects are discussed below.

Understanding the risk

When you see large breaches (four million records at the US Office of Management & Budget, 11 million records at VTech, etc), the data stolen can include social security numbers, employment history, search history and personal information (just think about our answers to common security questions). Hackers can use this information to commit identity fraud, create elaborate and sophisticated phishing schemes and gain even more valuable information along the way. Hacking techniques evolve rapidly and the 'good guys' are hard pressed to keep pace with the rate of change.

'Big data', or the hot trend in using faster and faster analytics to evaluate larger and larger sets of data to predict trends events, has become a tool for cybercriminals to rapidly mine information from hacks, and then to repackage and resell this information quickly.[13] As a case in point in May 2016, 427 million passwords of MySpace users were offered for sale for 6 bitcoins or about $2800.[14] Trading in bad debts has also become a large industry in the United States, often with very poor controls on the data transmitted or even substantiated as being valid debts. Debtor lists are another easy source of information, purchased for pennies on the dollar from banks and interim brokers, often consisting of just a simple Excel spreadsheet containing names, addresses, social security numbers and the debt information.[15] Taking this type of data – which, for MySpace or LinkedIn, may also include college or school affiliations, family relationships, friends, locations, photos and birthdates – a hacker can use the analytics available in order to quickly compile a profile of an individual, which can then be used for identity theft. Even more likely, the information is packaged and resold further up the criminal food-chain.

Indeed, identity theft may in fact become passé, with data breaches being increasingly used to identify targets for ransomware, where a virus (malware) can be installed on a computer which then locks down all files until the user pays a ransom to the malware operators to remove the restriction. Sometimes the system as a whole is locked; variants (the 'crypto-virology' forms of ransomware) encrypt all files on the system's hard drive, rendering them useless without the key. Ransomware has been noted as one of the most lucrative forms of cyber theft, generating an estimated 1,425% average return on investment for hackers, with the cash outlay being less than US$6,000 to obtain the necessary equipment and target lists.[16] When you consider that hackers can achieve these results from the comfort of their living room, in perhaps complete anonymity, and are often paid in bitcoins, which are untraceable, the allure of the scam becomes even clearer.

In 2016 we have started to see some alarming thefts at the sovereign nation level, most notably in February, when hackers issued instructions via the SWIFT[17] network to steal US$951 million from Bangladesh Bank (the central bank of Bangladesh). Some of the transactions succeeded, with US$20 million recovered from a wire to Sri Lanka and US$81 million to the Philippines before the Federal Reserve Bank of New York blocked the remaining US$850 million of transactions at the request of Bangladesh Bank.[18] SWIFT has since acknowledged that similar attacks have been attempted before and that the hackers were likely to have spent months inside the bank's computer system understanding how trades were placed and stealing the necessary authorisations.[19] Bloomberg reported that the investigation has found similar breaches at as many as 12 additional banks,[20] highlighting the systemic risk to the global financial system and the importance of shoring up any weak links.

For family offices and wealthy families who may place undue reliance on the cybersecurity initiatives of their investment firms, all of this was most unwelcome news.

Developing robust security protocols

The US Securities and Exchange Commission has made cybersecurity a top initiative and it is now a key component of examinations. They noted in a recent report that small and midsize businesses are the principal target of cybercrime.[21] Further, most businesses they examined that had cyber policies or IT security initiatives in place did not adequately address the risks faced by the business but were cobbled together from either standardised consultant offerings or developed internally by untrained individuals. Generally speaking, small and midsized businesses (SMBs) have less robust cyber defences and can be an easy gateway into larger organisations. The hack of Target from November 2013 was believed to have come into Target's systems through a

contractor, resulting in the theft of data relating to 70 million customers.[22] This vulnerability is not surprising since SMBs face the same threat landscape as larger organisations but have smaller (perhaps non-existent) IT teams and many have no cybersecurity protocols whatsoever.[23]

So how should a family office, or a wealthy family, begin to develop (or revise) its cybersecurity procedures? First, it is important to identify and understand the breadth and depth of the data at risk. To be most successful, the risk procedures developed need to work for the data and operations you have and need to mirror the existing workflows that are already in place. We usually begin a discussion in this area by breaking into the four arenas outlined at the start of this article:

- the family itself (and its actions with the outside world);
- the family office in relationship with the family;
- the family office in relationship with advisers; and
- the family office in relationship with investment managers or operators.

For each of these, we suggest mapping as many of the activities as possible and note that information can flow both ways. If information is received or downloaded from an encrypted source, the immediate step is often to save it to a local file and then, unfortunately, retransmit it in an unsecured fashion to another party. Most IT systems still operate in terms of a centralised server model, with computers linking into the central server; so cybersecurity initiatives often focus on keeping data secure and intact within a closed system. This may have worked 10 or more years ago but in a virtual work environment, where we are in constant email communication over insecure public networks, cybersecurity needs to be evaluated from the ground up and restructured to meet the demands of today's work environment.

The most important data to secure is personally identifiable information (PII) relating to the family, which might be held in the family office and/or in the multiplicity of places that this data is used or shared. PII includes anything where a name can be attached to another identifier – such as a social security number, a driving licence number, a financial account, a credit or debit card, a place of employment or (in the United States) information relating to the Health Insurance Portability and Accountability Act. Even getting partial chunks of information that may seem quite benign can be used to unlock other information. In a chilling article from 2012, Mat Honan, a columnist at *Wired* magazine, laid out how he had been hacked because small bits of PII were used to exploit loopholes in various technical support systems.[24] By getting a partial (four-digit) credit card number from Amazon, hackers were able to get Apple Technical Support to open his iCloud account and, from there, hackers erased all the data on his iPhone, iPad and laptop. Many security experts suggest using fake identifiers where possible and changing them by platform as a means of foiling people who seek to 'daisy-chain' their way into your systems by gaining access through one account.

In addition to securing PII, it is critical to secure all access points to the PII. Most breaches occur through lost or stolen equipment – for example, stolen laptops (behind many early identity thefts) and even smaller items such as flash drives (which might have files on them that have not been properly erased) – and so it is recommended that all peripherals be inventoried and disposed of properly (wiped and shredded by a professional). Businesses should be routinely checking all systems and peripherals for viruses or malware. On the basis that data breaches are often discovered several months after lurkers have been in a system and watching routines, protocols should be developed to break patterns or disrupt information flows, in an effort to stymie possible breaches. For family offices, this can be requiring password changes frequently, encouraging the use of external flash drives, a copy-and-paste approach to password log–ins when out of a secure network environment in an effort to bypass key-logging software, and carefully monitoring the cybersecurity efforts of key advisers and partners.

Any inventory that is compiled for developing security protocols should also include a review of the systems or routines used by the family office, including all points of access to information (inbound and outbound) and what information is stored in the cloud. Capturing this for the family can be difficult but not unmanageable. Total Digital Security, a cyber security consulting firm, recommends following a daily routine for a family to identify areas where security can be enhanced.[25] Simply noticing what information is being requested, the type of contact or social media that is used, and having some basic security procedures in place for family members in their communication and social media activities can drastically reduce the risks of cybersecurity breaches or identity theft.

Finally, cyber security is becoming a common addition to any RFP (request for proposal) process as family offices recognise the need to understand and evaluate a vendor's data protection and notification protocols. Remember that there are more than 1500 cybersecurity vendors in the United States alone and a large firm is likely to work with 60 or more of these firms in different roles. In this instance, complexity becomes the enemy of security. Many firms will consolidate or go out of business in the coming years and, simply put, when you have 60 or more relationships and none are stitched together, you have a recipe for disaster. What is the risk to a family office

The family office needs to be able to require all employees and family members, as well as outside advisers or consultants, to adhere to whatever risk protocols the family office has identified as necessary in order to minimise the occurrence or extent of a security breach.

if data is breached at a vendor, and can it infiltrate the family office systems through daily data feeds? Some businesses have developed a checklist to review relevant matters with any partners or external vendors, to ensure the business understands and reviews data collection practices and cyber initiatives at these firms. Do they have cyber insurance? Would the family office be able to recover if there was a breach? What notification requirements exist? What policies are in place to monitor systems for breaches? These are all important questions to which satisfactory answers need to be given.

Deliberate breaches may be a bigger but uncontrollable issue; a deliberate breach is one where a disgruntled employee steals or posts data. Since a family office is often highly leveraged through the use of its outside providers, it is likely that any disgruntled employee is outside the control of the family office and lurking within a large corporation or vendor. Morgan Stanley had a private wealth management executive who stole and purportedly posted data on up to 10% of the firm's 3.5 million clients.[26] Your partners and investment advisers are required to have accurate PII, and so providing false birthdates or other information that might work for a random website is not really an option here. Instead, the family office team needs to understand what information has been shared, and have a sense of where that information has been further shared by the advisers (eg, an investment adviser is likely to have passed at least some information on to a discrete portfolio manager, who may be using a different clearing house, or master custodian, or reporting system – all of which are potentially vulnerable to data breaches). Knowing what information is out in the world, and how it can be tracked, is important in developing a protocol. Then, using this knowledge to develop the means to test security becomes the challenge. Essentially, you will be hacked and the information is probably already out in the public domain, so how can you prevent additional information from seeping out becomes the question when developing these protocols.

One area of concern for many family offices is the routine transmission of information to family members for investment reviews or family meetings. If the family is travelling to an annual meeting, often there are policies in place as to how material must be transported (always in hand luggage, never transported as we will provide hard copies on arrival, etc). Some family offices and corporate boards have tried to minimise information transmission through requiring all communication of a sensitive nature to be sent through private email domains, secure vaults and encrypted emails. Others have moved entirely to sending out data on dedicated tablets loaded with relevant information for the family meeting or board retreat; these tablets are then collected, notes stored and data wiped, after every meeting.

Email is often the most difficult medium to control, followed closely by instant messaging. Here, the use of private email domains and secure networks is probably the best defence. One area that is often overlooked by families and family offices is the retransmission of encrypted or secure files over an insecure network. I might receive a note from my attorney and I immediately flip it to my family business consultant for her input, doing so from my iPhone while waiting in an airport. I think I am being efficient and inclusive! However, not only have I voided the attorney–client privilege and made the information discoverable in a legal case, but it is also likely that I have allowed any attachment to become infected or misdirected. Education here is critical, so family members, family office employees and your partners must all understand the risks associated with transmitting data.

Family members and employees must become active participants in the management of information security, both at home and in the workplace. The 'human factor' mistake is the biggest risk – opening a seemingly legitimate email and clicking on the links, or downloading the material attached. Family offices should consider developing (or revamping) an information security policy (ISP) that can be used to monitor information transfers and, hopefully, minimise the risk of unacceptable use of websites, information and data transfers within the family

office and by family members. While it may be tempting to focus on the younger family members – the so-called 'digital natives' who have never lived without email, the internet, social networks or ubiquitous mobile devices – cyber fraud research shows that senior family members lose up to $36 billion annually in total to cyber theft. It is estimated that 37% of seniors are affected by financial abuse in any five-year period. While a portion of this is allocable to more normal forms of fraud, such as abuse by caregivers or trusted advisers, increasingly it is taking the form of identity theft and online scams (think Nigerian princes seeking your help!).[27] Identity theft is one of the top complaints with the Federal Trade Commission (FTC) in the United States, often related to taxpayer identity theft and fraud; and the 'mature' market (denoted as aged 50 or older!) is the single largest demographic for identity theft and fraud, with Florida, Georgia, California, Arizona and Texas having the highest incidence. Children aged 19 and under were the second-largest demographic.[28]

Looking forward, as we become more and more connected and our 'internet of things' allows us to access any device from anywhere, cyber crime will undoubtedly target cars, home security systems, heating and cooling devices, and medical devices – causing another headache for the family office cybersecurity chief![29]

Ensuring continued protection

Getting started

While a full risk assessment in readiness for setting up security protocols can be time consuming and require the hiring of experts, there are many steps that a family office can take immediately which should reduce risk significantly. The following are worth noting:

- *Hide in plain sight:* A simple screen protector, often less than US$20 on Amazon, can shield your tablet, laptop or other device from prying eyes. Next time you are on a plane or train, walk up the aisle half way through the trip and notice how many screens you can read from several seats away (and how few people notice that you are looking over their shoulder!). This can be an easy way to ensure your more obvious information is not grabbed.
- *Check and double check:* Use two-factor authentication whenever possible. Many financial institutions and the like offer an option for a two-factor authentication, which would require you to receive a text message or other code at every log-in.
- *Expect permanence:* What is the difference between email and true love? Email lasts forever! It is not far-fetched to expect that in a few years every digital voicemail, text and email could be online and text-searchable. If its discoverable in a lawsuit, you should expect that hackers will be there first. If you are transmitting sensitive information, use an old-fashioned person-to-person call.
- *Avoid peeping Toms:* Use a Post-It note or similar to cover the camera on every device. They can be easily hacked to turn on and see the surroundings. Most devices do not have any warning light to indicate that the camera is active.
- *Go private:* Families and family offices should establish a private (ie, not Gmail. Microsoft or Yahoo) email domain name and have all traffic through a secure server.
- *Swap 'em out:* We all groan when asked to create a password and often reuse the same one for multiple services. Passwords should ideally be at least 10 characters (14 or more is ideal) and should be a mix of numbers and letters. If memorising them is too hard, try using a sentence and switching numbers in for letters. "Chocolate is Great" becomes "Ch0c018izGr8" – hard to hack but easy to remember! Scheduling a change of passwords with the solstice, on your birthday etc will ensure you do not keep the same password in place for more than a year, ideally no more than three to six months. Note that password keepers may be helpful but have been hacked and an old-fashioned paper system is often the most secure way to keep track of log-ins. Wherever possible, use a new or substantially different password on every website or login.
- *Clean it up:* We are all digital hoarders, cluttering up our systems and peripherals with lots of old (often duplicate) documents. Taking time to clean up and remove unused software and duplicate files, as well as running good anti-virus software, should be a routine occurrence.
- *Close it down:* Extend your clean-up procedures to shutting down old email accounts and reviewing your social media profiles for privacy settings, and remove things that may be

Email is often the most difficult medium to control, followed closely by instant messaging.

identifiers of location, background information (where you went to school, home town, etc). Where possible, have your financial institutions close any unused accounts.

- *Lock it up:* Augment your routine clean-up by running a formal credit check on every family member at least annually. This is a good way of monitoring for fraud on younger or older family members who are the prime targets of credit theft. If possible, freeze all of the credit accounts and just bear in mind that this action requires an affirmative unlocking mechanism (usually spanning 24 hours) for any credit checks or the opening of new charge accounts. Many US family offices file IRS Form 14039 to lock files with the IRS as well.
- *Travel wisely:* When travelling domestically, always use a virtual private network and never ever use public or communal Wi-Fi systems. When travelling internationally, many families use 'loaner' or 'travel' devices that are erased when they leave their home jurisdiction and wiped clean when they return (and definitely before you upload files into the system on your return). Depending on where you travel internationally, you may want to disable all Bluetooth and Wi-Fi facilities on your mobile devices, keep your phone in sight at all times and even consider copying and pasting passwords from a (clean) flash drive rather than typing them in, to foil key-logging software that can often be installed surreptitiously by hackers.

Finding good advisers to help you through the processes described above, and to take you further into designing your protocols, can be very valuable. One of the key complaints made by cybersecurity experts is that many of the experts in the field come from a tech or military background and lack the ability to look across multiple platforms and understand business flows outside their own area of expertise. For family offices and wealthy families, your cyber advisers should have a keen understanding of your operational issues and the myriad considerations that drive your operations. It helps, too, if they have a realistic approach to protecting families and the data in the family office. The best systems are only as good as the weakest user; so if a family member is going to insist on using a Gmail account, the family office needs to take this into account in designing its protocols.

Testing the systems

On average, there is more than one disaster declared every week in the United States.[30] Family offices should develop a broad incident response plan for any type of security breach and test the plan at least annually. We recommend considering all types of situation. What if there is no internet access (think Hurricane Sandy, which knocked out lower Manhattan, much of Connecticut and New Jersey and large areas around Philadelphia), or what if there is no physical access to the office but you have access to data? What if you were the victim of ransomware and had no access to the data on your own devices? Or what if there was a massive cyber attack that brought down the electrical and communications grid? (We have moved so far to a paperless society that much of our recordkeeping could be lost in this last type of event.) It is critical to determine how resilient the family office and the family itself can be to disaster and disruption, and to the hacking or hijacking of its information.

Finally, like shampoo instructions, it is important to 'lather, rinse and repeat'. Developing a great system may only work for a few years (if we are lucky) until it is outdated. Testing the system annually and being willing to take it apart, or bring in experts to evaluate the system on a regular basis, is critical to staying abreast of technological developments.

Dealing with a data breach

In the United States (as well as many other developed countries) there are several laws requiring notification of security breaches.[31] However, there may be a delay between when the breach is detected and when an individual or firm is notified, even if there are headlines about the initial breach. Hackers are routinely targeting financial institutions and hospitals or healthcare networks (eg, Anthem Network) but large retailers (Home Depot, Lowes) are also at risk. Unfortunately, the hackers have often been in the system for 200 days or more by the time the breach is detected.

In May 2016 alone, breaches were noted by several leading social networking sites. Reddit reset passwords of 100,000 users in response to account hijackings. LinkedIn was forced to reset the passwords of more than 100 million users who had created accounts prior to 2012 and not changed their passwords since then. The hack was not even noted internally but the company was alerted to the offering for sale of a database containing LinkedIn credentials from a 2012 data breach. While accessing your Facebook or Reddit history might not seem to hold much information, the ability to mine this data and aggregate information can make seemingly disparate information quite valuable. Also of note in May 2016, Microsoft announced it would take affirmative action to block account holders using simple or common passwords and passwords that had been exposed on data breach lists.[32]

When you are notified of a breach, whether by an external vendor or by your own internal risk

management systems, it is important to immediately evaluate what was taken or lost, and what might have happened to this data since it was taken or lost. Who might have this data and what might they do with it? From here, the process diverges:

- If the breach was of your internal systems, risk controls need to focus on how it happened and what actions can be taken to further protect information.
- If the breach was internal in some other way, you need to evaluate your data controls and whether you have notification responsibilities out to your clients or other vendors.
- If the breach was external and your data was stolen from someone else's system, determine whether there is any remuneration or support being provided. Sometimes there are credit monitoring systems which are offered to victims of the breach; at other times you or the firm that was breached may have cyber liability insurance that can offset (potentially) the costs you may face in taking steps to secure your data again.

Final comment

The best approach to cybersecurity is to assume that the barriers safeguarding your data have already been breached and that you will be the target of ransomware or identity theft. Assume that your investment partners have already been breached as well. Build your scenario planning from here and use it as an exercise in family gatherings. Educate your family members and even your business partners about the issues presented, and encourage their input into your policies and procedures. The best defence is a good offence and, if thoughtful and carefully prepared procedures are in place, the cost and disruption of this unfortunate new reality can be minimised.

Holly Isdale is the founder of Wealthaven, a consulting practice focused on family succession and family office operations. She has been writing and speaking for many years on estate and financial planning matters but, as the child, spouse and mother in a family of engineers, her devotion to and fascination with all things technical has manifested itself in writing and consulting on topics of cybersecurity, digital asset protection (and digital death) and gamification. The current article is intended for educational purposes only.

1 See http://fortune.com/sony-hack-part-1/.
2 See https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach.
3 See www.anthemfacts.com/.
4 See www.horizonblue.com/about-us/news/alerts/information-about-premera-security-breach.
5 See www.techtimes.com/articles/88658/20150926/hilton-branded-hotel-properties-hacked-clients-credit-card-data-compromised.htm.
6 See www.ibtimes.com/mandarin-oriental-hacked-luxury-hotel-chain-admits-credit-card-numbers-were-stolen-1836574.
7 See http://money.cnn.com/2015/09/30/technology/trump-hotels-hack/index.html.
8 See www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/.
9 See www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge/.
10 See http://cybersecurityventures.com/cybersecurity-market-report/.
11 See www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-020/#3c69faf22191.
12 See www.pwc.com/gx/en/issues/cyber-security/information-security-survey/key-findings.html.
13 See www.gartner.com/newsroom/id/2663015.
14 See www.technewsworld.com/story/83575.html.
15 See http://loanmls.com/content/buy-bad-debts.html.
16 See www2.trustwave.com/GSR2016Success.html?aliId=85969971.
17 SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, was thought to be a super-secure system that is used to authorise interbank payments.
18 See http://nypost.com/2016/03/22/congresswoman-wants-probe-of-brazen-81m-theft-from-new-york-fed/.
19 See www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html?_r=0 ; http://www.wsj.com/articles/hackers-in-bangladesh-bank-account-heist-part-of-larger-breach-1458582678.
20 See www.bloomberg.com/news/articles/2016-05-26/swift-hack-probe-expands-to-up-to-dozen-banks-beyond-bangladesh
21 See www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html.
22 www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html
23 https://business.timewarnercable.com/resource-center/news/national-small-business-survey-press-release-twcbc.html.
24 See www.wired.com/2012/08/apple-amazon-mat-honan-hacking/.
25 See www.totaldigitalsecurity.com/blog/a-day-in-the-life-of-a-family-protected-by-total-digital-security.
26 See www.reuters.com/article/us-morgan-stanley-breach-plea-idUSKCN0RL22920150921.
27 See www.truelinkfinancial.com/news/latest-report-elder-financial-abuse-true-link-finds-36-48-billion-lost-annually-seniors/.
28 See http://amac.us/senior-id-theft-top-ftc-consumer-complaint/.
29 See www.csoonline.com/article/2984193/cyber-attacks-espionage/new-cybercrime-wave-drives-iot-security-spending.html.
30 See www.fema.gov/disasters/grid/year.
31 US federal laws include: the Financial Services Modernization Act of 1999 (known as the Gram-Leach-Bliley Act (GLBA)); the FTC's Fair Credit Reporting Act (FCRA); the Federal 'Red Flag' Rules (16 CFR 681.1); the Health Insurance Portability & Accountability Act (HIPAA); and the Hitech Act of 2009. In the United States, furthermore, the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) have a major cybersecurity initiative in place for investment firms. In addition, at least 46 states have enacted some type of legislation relating to security breaches.
32 See www.technewsworld.com/story/83575.html.