CYBERSECURITY:

STAYING SAFE IN A PERILOUS WORLD

SEI New ways. New answers.*

seic.com/ims
Financial institutions are a favorite target of hackers and cybercriminals.

Faced with increasingly sophisticated threats, what can asset managers do to keep their assets and investors safe? Is it an arms race, or is there a better way?
Contents

A dangerous environment ........................................... 2

Threat level .................................................................. 3

Uneasy investors .......................................................... 5

The state of play .......................................................... 6

Preparing for the inevitable .......................................... 7

Planning and implementation ....................................... 9

Implications for asset managers .................................. 13

About the survey ......................................................... 15

About SEI ................................................................. 16

Sources ..................................................................... 17
A DANGEROUS ENVIRONMENT

If there were any lingering doubts that cybersecurity is a serious issue with profound consequences, these were quickly dispelled by the 2016 presidential election. Regardless of the degree to which hacks and leaks played a role in ultimately deciding the winners and losers of that contest, it should now be clear to everyone that the cyberlandscape is one where very real battles take place daily.

Cybersecurity is a growing problem for all businesses, and the scale is staggering.

Cybercrime costs the global economy an estimated $500 billion annually.¹ In the United States alone, companies with more than 1,000 employees suffer an average loss of more than $15 million annually.² The Identity Theft Resource Center notes that nearly 178 million personal records were exposed in data breaches in 2015; Yahoo announced it has suffered data breaches of 500 million and more than 1 billion accounts in separate instances.³

Painful as they may be, direct costs are likely to pale in comparison to indirect losses, such as the loss of trust or the cost of remediation work required to thoroughly clean systems after a breach.⁴ Cybersecurity has become a top priority for business leaders, with CEOs expressing extreme concern about the potential for cyberthreats to stunt business growth.⁵

None of this is likely to be news to large financial firms that have long been targeted by cybercriminals, but it has served as a wakeup call for smaller organizations and those in less active corners of the financial services ecosystem that have done little to develop or implement countermeasures. As is often the case with technology and innovation, financial firms lag behind many other types of companies in risk management awareness and protocols, making it even more concerning that, according to PricewaterhouseCoopers (PwC), financial institutions are more than 30% more likely to be targeted by cybercrime.⁶

Breaches in highly regulated industries tend to be especially costly, and the financial services sector is a prime example.⁷ This fact has been underscored by former U.S. Securities and Exchange Commission (SEC) Chair, Mary Jo White, who repeatedly emphasized the importance of cybersecurity on numerous occasions, remarking, “We can’t do enough in this sector,” “Cybersecurity … is one of the greatest risks facing the financial services industry,” and “It is imperative we continue to enhance our coordinated approach to cybersecurity policy.”⁸

A number of factors are accelerating the growth of cyberthreats to asset managers specifically. The well-documented industrywide trend toward greater transparency, providing data and information more often and through a variety of means, has had the unintended consequence of greatly expanding the scope of information trading hands, thereby spreading vulnerability. The proliferation of mobile devices multiplies vulnerability exponentially. The growing reliance on service providers—while often done for extremely good reasons—also expands the risk perimeter that needs to be protected, particularly if they are not properly integrated into a firm’s cybersecurity plan.

How well is the asset management industry responding? SEI surveyed a range of asset management firms in late 2016 in order to better understand how people are responding to the evolving threat. Our research suggests that most cybersecurity efforts, while well-intentioned, have not kept up with the scale, frequency, variety, or ingenuity of threats. Asset management firms now run the gamut from those that are woefully uninformed and underprepared to those that lead the way with integrated cybersecurity programs that span entire ecosystems across the globe.
Unsurprisingly, there is unanimous agreement among those responding to the survey that cyberattacks pose a threat, but how much of a threat they pose depends to some degree on who is asked. Almost three out of 10 diversified asset management firms, for example, characterize cyberattacks as a significant threat, while the remainder considers them to be a moderate threat (Figure 1). Private equity (PE) firms, on the other hand, are less likely to view hacking as a major risk.

It is also instructive to look at the retail banking industry, which is arguably further along the path of understanding and dealing with cybersecurity. This sensitivity can be traced in part to the sheer amount and size of the risk as well as potential threats to individual investors. It is also likely to be due to the fact that the industry is being disrupted more quickly by fintech firms. Regulatory compliance is easily top of mind for these firms, but cybersecurity ranks among other significant challenges, such as customer service and staffing.  

**FIGURE 1**
How big of a threat do cyberattacks pose to your firm?

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Diversified</th>
<th>PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Significant threat</td>
<td>79%</td>
<td>71%</td>
<td>89%</td>
</tr>
<tr>
<td>Modest threat</td>
<td>21%</td>
<td>29%</td>
<td>11%</td>
</tr>
</tbody>
</table>

Source: 2016 SEI Cybersecurity Survey.

The threat of cyberattacks is more than vaguely ominous. Individuals tasked with cybersecurity say they are concerned about a variety of specific ways in which their firms could be harmed. First and foremost among these is the potential damage done to a firm’s reputation. After all, the fact that an attack was successful at all may be more harmful to a manager than the actual damage done by a breach. More than half of all respondents are “very concerned” that digital breaches could dent their reputation or worse (Figure 2). Dissatisfied clients are another major concern, followed by regulatory compliance and competitive vulnerability. Perhaps surprisingly, the potential economic impact of a breach is least likely to be a major concern for asset managers.

Risks are not limited to direct costs associated with an actual attack. Regulatory risk is a good example. As mentioned earlier, the SEC is already prioritizing cybersecurity. Other regulations and guidelines shaping the cybersecurity landscape in the U.S. include FINRA, the Department of Justice, and the International Organization for Standardization (ISO). Financial Conduct Authority (FCA) rules cover managers in the U.K., and the EU is expected to introduce General Data Protection Regulation (GDPR) standards in 2018. Firms can make themselves vulnerable to enforcement actions simply by failing to do any number of things, including enforcing policies, conducting periodic assessments, responding to identified deficiencies, protecting customer information, or having adequate policies, procedures or protections regarding vendors and outsourcing.
It is tempting to think that theft is the only motivation for cybercrime, but crime may not even be the main objective. Some perpetrators are primarily interested in sowing the seeds of confusion and terror. Others may be aiming for revenge. Competitive intelligence and intellectual property are also proven motivators.

If money is indeed the goal, there are several ways of accomplishing the theft. One of the oldest forms of cybercrime is the reselling of personal data or credit card details. Fraudulent transfers have also worked in the past. A more recent phenomenon known as ransomware involves disrupting business operations with a type of malware called CryptoLocker until a ransom is paid.

Many people may have a mental image of young hackers operating independently and wreaking havoc from the safety of their basement bedrooms, but the reality is that there is a growing array of bad actors who possess increasingly sophisticated tools and are driven by a variety of motives. Organized crime syndicates hailing from many countries are no longer limited by physical boundaries and now have the ability to operate on a global scale. State-sponsored hackers also have global reach, although their motivation is likely to be political leverage rather than monetary gain. Corporations engage in espionage to undermine competitors or learn their secrets. Terrorists terrorize. The aforementioned young basement dwellers might be motivated by money, but they may also be doing it for kicks (aka “lolz” in online parlance), just because they can or, in the case of more idealistic “hacktivists,” to score political points. Yet, the most common perpetrators may be employees. While sometimes malicious (e.g., theft or revenge), breaches traced back to employees are more likely to result from carelessness, poor training, badly designed procedures, or inadvertent lapses.
UNEASY INVESTORS

Asset management firms face this diverse range of threats because they are, in the words of a famous bank robber, “where the money is.” They may not store cash in vaults, but asset management firms are vast repositories of valuable data that can potentially be exchanged for hard currency or used as leverage to further a different goal. Sensitive assets include investor data, employee data, and intellectual property such as trading algorithms or proprietary research.

Acutely aware of these risks, many institutional investors are increasingly likely to make cybersecurity an important part of their manager selection and due diligence process. Fund managers are beginning to hear more from concerned investors, fueling their drive to demonstrably make their assets and data safer. One out of three survey respondents say cybersecurity is very important to their investors, and another 61% agree that it is important (Figure 3). It is interesting to note that Asian investors appear to be the most concerned, followed by those in Europe.

Growing concern among investors is in many cases reflected in more focused and thorough due diligence. More than eight out of 10 respondents say investors have been paying more attention in recent years to cybersecurity while conducting operational due diligence (Figure 4). This greater scrutiny is particularly acute at larger firms: 60% of firms with more than $1 billion of assets say there is much more attention being paid to cybersecurity during the due diligence process. This is consistent with the experience of SEI, which has seen a growing number of cyber-related questions in RFPs from asset managers over the past several years. While it may be surprising that 20% of U.S.-based respondents indicated that cybersecurity was not important to their investors, this may simply reflect an assumption on their part that a basic level of security is already in place. It seems safe to say that managers do indeed take the topic seriously.

FIGURE 3
How important is your firm’s cybersecurity to prospective investors?

<table>
<thead>
<tr>
<th>Region</th>
<th>Very important</th>
<th>Important</th>
<th>Not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>32%</td>
<td>61%</td>
<td>8%</td>
</tr>
<tr>
<td>U.S.</td>
<td>27%</td>
<td>53%</td>
<td>20%</td>
</tr>
<tr>
<td>Europe and U.K.</td>
<td>50%</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>Asia</td>
<td>67%</td>
<td>33%</td>
<td></td>
</tr>
</tbody>
</table>

Note: Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.

FIGURE 4
Have you seen a change over the past few years in the attention paid to cybersecurity during the operational due diligence process?

<table>
<thead>
<tr>
<th>Category</th>
<th>Much more attention</th>
<th>Some additional attention</th>
<th>Little change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>29%</td>
<td>55%</td>
<td>16%</td>
</tr>
<tr>
<td>AUM &gt; $1B</td>
<td>60%</td>
<td>30%</td>
<td>10%</td>
</tr>
<tr>
<td>AUM &lt; $1B</td>
<td>17%</td>
<td>58%</td>
<td>25%</td>
</tr>
<tr>
<td>Diversified</td>
<td>28%</td>
<td>50%</td>
<td>22%</td>
</tr>
<tr>
<td>PE</td>
<td>28%</td>
<td>50%</td>
<td>22%</td>
</tr>
</tbody>
</table>

Note: Excludes “Don’t Know.” Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.
Despite widespread concern, it would be fair to say that there are a significant number of money management firms for whom cybersecurity is not yet a critical priority. This may be, in part, because it remains a theoretical threat for many. Three out of four firms in the survey say they have never been the victim of a successful cyberattack (Figure 5). Most of the rest have had their defenses breached between one and five times, while a small minority report six or more breaches.

**FIGURE 5**
How many known cybersecurity breaches has your firm experienced in the past five years?

<table>
<thead>
<tr>
<th>Total</th>
<th>74%</th>
<th>23%</th>
<th>3%</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>71%</td>
<td>29%</td>
<td></td>
</tr>
<tr>
<td>Europe and U.K.</td>
<td>75%</td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>Asia</td>
<td>50%</td>
<td>25%</td>
<td></td>
</tr>
</tbody>
</table>

Note: Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.

Other surveys have found a higher incidence of attacks, possibly due to differing definitions. One study reported that 70% of PE firms experienced three or more cyber issues in the past year alone, while 29% of firms experienced five or more issues during the same time frame.\(^\text{16}\) It is worth noting that research of this type is likely to underreport the actual extent of the problem. Beyond an understandable reluctance to admit weakness, it is not unusual for breaches to go undetected for weeks, months, or even indefinitely.

Cybersecurity issues regularly experienced by investment firms include malware, worms and viruses, unauthorized access to corporate data, and hijacking of social media accounts.\(^\text{12}\) How is data accessed? Common methods include phishing, friending, stealing passwords, or physically following employees into offices. Half of all survey participants reported incidents of vandalism or business interruption in which no theft actually took place (Figure 6). Although it is tempting to think of these types of attacks as relatively minor, they can take a long time to resolve, resulting in high costs. Costs stemming from business disruption are actually higher than those associated with data theft or revenue loss.\(^\text{15}\) Those originating with malicious insiders can take an average of more than two months to resolve, compared to viruses or botnets, which are likely to be detected and dealt with within a few days.\(^\text{14}\)

**FIGURE 6**
What types of attacks has your firm experienced? (Choose all that apply)

| Vandalism | 50% |
| Ransomware | 29% |
| Employee data theft | 14% |
| Investor data theft | 7% |
| Intellectual property theft | 7% |

Source: 2016 SEI Cybersecurity Survey.
Underscoring a form of cybercrime that has soared in popularity in recent years, 29% of firms have experienced ransomware attacks, in which their systems were infected by software designed to disrupt operations until money was paid to the attacker. Employee data has been stolen at another 14% of firms. Investor data and intellectual property are stolen less often, with only 7% of firms reporting being victimized in this way. Adding an extra layer of complexity for firms drawing up a cybersecurity strategy, each type of attack is more likely to target different parts of an organization. While malicious software may primarily affect the finance or portfolio management functions, phishing or social engineering attacks are more likely to have repercussions for the compliance and legal functions.15

PREPARING FOR THE INEVITABLE

The inimitable Benjamin Franklin once said “By failing to prepare, you are preparing to fail.” He may as well have been speaking about cybersecurity, where preparedness is absolutely vital. Traditional models are now insufficient and more sophisticated; proactive efforts will be required to become effective and resilient in an evolving threat environment. Most asset managers nominally recognize the need for proper policies and procedures, but the level of true preparedness inevitably varies widely.16

For firms looking to improve their cybersecurity capabilities, it is important to recognize that risk cannot be entirely eliminated and that it is not a matter of if you will be attacked, but when.17 It is also true that bad actors will constantly rewrite their playbooks, devising new ways to reach their objectives. While many firms have already spent significant sums on protecting themselves, they may now want to reorient their efforts toward detection and resolution.18 As noted by the FBI, companies should be prepared to be hacked repeatedly.19

Cybersecurity should also be considered in the context of overall security. It might surprise people to know that many digital breaches begin with physical access.20 Cybersecurity is ultimately just one part of a holistic data protection plan featuring policies, procedures, checks, firewalls, and redundancy. Whether physical or digital, firms need to know where all their data is being stored, processed, and transferred so that they can implement appropriate controls that “travel with the data.”21

Based on our survey responses, preparations by investment firms to date have not been overly aggressive. Only 13% of survey respondents feel their firms are extremely well prepared to meet cybersecurity challenges. This is, incidentally, the same proportion that feels they are not at all prepared (Figure 7). Three out of four claim their firms are somewhat prepared, but this can vary dramatically. British and European firms, for example, are far more confident about their preparedness than their peers in Asia. Larger firms are also more likely to be prepared than smaller ones.

FIGURE 7

How well prepared is your firm to meet cybersecurity challenges?

<table>
<thead>
<tr>
<th></th>
<th>Extremely well prepared</th>
<th>Somewhat prepared</th>
<th>Not at all prepared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>13%</td>
<td>74%</td>
<td>13%</td>
</tr>
<tr>
<td>U.S.</td>
<td>13%</td>
<td>73%</td>
<td>13%</td>
</tr>
<tr>
<td>Europe and U.K.</td>
<td>17%</td>
<td>83%</td>
<td>13%</td>
</tr>
<tr>
<td>Asia</td>
<td>17%</td>
<td>50%</td>
<td>33%</td>
</tr>
<tr>
<td>AUM &gt; $1B</td>
<td>20%</td>
<td>70%</td>
<td>10%</td>
</tr>
<tr>
<td>AUM &lt; $1B</td>
<td>8%</td>
<td>69%</td>
<td>23%</td>
</tr>
<tr>
<td>Diversified</td>
<td>5%</td>
<td>74%</td>
<td>21%</td>
</tr>
<tr>
<td>PE</td>
<td>5%</td>
<td>74%</td>
<td>21%</td>
</tr>
</tbody>
</table>

Note: Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.
If PE firms are relatively sanguine, it is not necessarily because they are better prepared. According to a 2016 Eze Castle survey, two-thirds of PE firms expressed confidence in their cybersecurity preparedness, but our research showed they are significantly less likely than diversified firms to claim they are “extremely well prepared.” More than one out of five PE firms goes so far as to say that they are not at all prepared to meet cybersecurity challenges. PE firms face an additional challenge: In addition to ensuring the safety and resilience of their own data, they need to keep an eye on the security of their portfolio companies. As daunting as that task seems, it may have a silver lining. Cybersecurity best practices could potentially be shared across portfolio companies, reducing development costs and streamlining implementation.

Given the fact that many firms have yet to find themselves on the receiving end of a successful cyberattack, it comes as little surprise to find that fewer than one out of three have ever practiced for a cybersecurity incident (Figure 8). A rehearsal of this kind is not unusual when it comes to general business continuity and disaster recovery, but has yet to become a feature of cybersecurity measures.

The most advanced firms bring a war game approach to simulations, purposefully introducing complexity and unpredictability in an effort to be better prepared for the unexpected. Drills of this kind can also highlight deficiencies in many aspects of a firm’s plan, ranging from vendor management to investor communications. Furthermore, simulations underscore the significance of prioritization. Not everything can be protected equally, so it is important to identify the digital assets that are most critical (e.g., those that would put you out of business if compromised) and deserving of attention and resources.

Vulnerability stemming from a lack of preparation may be exacerbated by another common shortcoming. Despite the fact that almost all money management firms operate within a web of counterparties and service providers, few have cybersecurity plans in place that cover these external entities. Four out of ten firms say their plans cover fund administrators, but it is relatively rare that this coverage extends to custodians, distribution platforms, prime brokers, or others (Figure 9).

It is critical for investment firms to first recognize the expanded risk perimeter that goes far beyond their own walls and servers. A security plan is only as strong as its weakest point, meaning coverage must extend to include all entities within a firm’s orbit. Unfortunately it is not unusual for investment firms to rely on third parties for security rather than extending their own plan outward. As some high profile incidents have illustrated, this can be a recipe for disaster. A proactive approach that integrates vendor initiatives with a firm’s own initiatives is much more likely to be successful. With this in mind, asset managers should evaluate existing and prospective vendors and partners for vulnerability, data handling practices, recovery plans, response times, and other metrics.
FIGURE 9
Which external entities does your firm’s digital security plan cover? (Choose all that apply)

<table>
<thead>
<tr>
<th>Entity</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fund administrator(s)</td>
<td>40%</td>
</tr>
<tr>
<td>Custodians</td>
<td>20%</td>
</tr>
<tr>
<td>Distribution platforms</td>
<td>12%</td>
</tr>
<tr>
<td>Prime broker(s)</td>
<td>4%</td>
</tr>
<tr>
<td>Transfer agents</td>
<td>4%</td>
</tr>
<tr>
<td>Broker dealer(s)</td>
<td>0%</td>
</tr>
</tbody>
</table>

Note: Excludes firms without plans.
Source: 2016 SEI Cybersecurity Survey.

PLANNING AND IMPLEMENTATION

Awareness and preparation are only truly effective when backed by a thoughtful, comprehensive, and carefully documented security plan. The plan should be backed by senior management and managed by a capable individual with a sufficiently broad mandate. Many (especially smaller) investment firms employ few technology specialists, making it difficult for them to adequately assess their vulnerabilities or design an effective security plan.

Retaining specialists from the outside is therefore the most common approach taken when developing cybersecurity plans. With expertise that reaches from overall vision down to tactical recommendations, external consultants are hired by two-thirds of all firms surveyed to produce cybersecurity plans (Figure 10). More than half of these subsequently moved the management of their cybersecurity plan in-house, while the rest rely on external parties to implement and manage the plan. In-house development is relatively rare.

FIGURE 10
Which best describes your firm’s cybersecurity plan?

<table>
<thead>
<tr>
<th>Category</th>
<th>Developed externally and managed in-house</th>
<th>Developed and managed externally</th>
<th>Developed and managed in-house</th>
<th>No cybersecurity plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>39%</td>
<td>27%</td>
<td>12%</td>
<td>21%</td>
</tr>
<tr>
<td>U.S.</td>
<td>47%</td>
<td>20%</td>
<td>20%</td>
<td>13%</td>
</tr>
<tr>
<td>Europe and U.K.</td>
<td>40%</td>
<td>40%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>Asia</td>
<td>25%</td>
<td>25%</td>
<td>50%</td>
<td>20%</td>
</tr>
<tr>
<td>AUM &gt; $1B</td>
<td>60%</td>
<td>15%</td>
<td>30%</td>
<td>10%</td>
</tr>
<tr>
<td>AUM &lt; $1B</td>
<td>31%</td>
<td>23%</td>
<td>15%</td>
<td>31%</td>
</tr>
<tr>
<td>Diversified</td>
<td>71%</td>
<td>28%</td>
<td>11%</td>
<td>14%</td>
</tr>
<tr>
<td>PE</td>
<td>33%</td>
<td>28%</td>
<td>11%</td>
<td>28%</td>
</tr>
</tbody>
</table>

Note: Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.

Most surprising is the fact that one out of five firms report having no plan at all. This group consists entirely of smaller firms with less than $1 billion in assets. They are mostly likely to be found in Asia and are twice as likely to be PE firms rather than diversified asset managers. Many of these firms also have no training in place for employees to learn about digital security issues and protocols (Figure 11). Annual training sessions can be found at 40% of firms, while another one in four trains people on a quarterly or monthly basis. Other firms report training employees “occasionally,” “periodically,” or as part of their new employee orientation and onboarding process.
Even at firms that have taken the time to develop and implement cybersecurity plans, it is extremely rare for those plans to have been recorded very well (Figure 12). Most survey respondents rate their plans’ documentation as good, but a sizeable minority says the clarity, detail, and comprehensiveness of their plans is only fair or even poor.

Many of these gaps or deficiencies can be put down to the fact that very few asset management firms have employees dedicated to cybersecurity. Only 10% of firms with more than $1 billion of assets report having a chief information security officer (CISO) on their payroll (Figure 13). It is most common among these larger firms to put chief operating officers (COOs) in charge, while chief technology officers (CTOs) are the next most common choice. There are no CISOs at smaller firms, where network administrators are as likely as COOs or chief financial officers (CFOs) to be placed in charge. It does not help matters that cybersecurity expertise is not widespread, making it difficult for many firms to locate or compete for scarce talent.

It is not uncommon for IT teams to be understaffed and focused on aspects of technology other than security. What makes it so potentially troublesome is when cybersecurity efforts are led by an individual who—no matter how senior—is likely to have many other (important and time-consuming) obligations. A separate survey found CTOs are almost universally responsible for cybersecurity at PE firms, including large ones.24 This might sound promising on the surface, but it is entirely possible that these professionals have skeletal teams reporting to them. On the bright side, this same survey found that 93% of PE firms believe their top IT executive is becoming more important, and 85% see them becoming more involved in helping meet regulatory and compliance demands.25
Cybersecurity insurance is a growing phenomenon, but it remains relatively rare. More than two-thirds of the firms in the survey do not currently have insurance (Figure 14), although fund administrators or other parties that provide outsourced services to investment managers often carry network security and privacy liability insurance and/or require such insurance of their vendor partners as an extra layer of protection. PE firms are much more likely than diversified managers to be operating without cybersecurity policies in place. A significant number of firms with insurance only purchased their policies within the last year, but larger firms are more likely to have been early adopters. Quantifying the actuarial risk of cyberattacks is a work in progress, but insurers are now covering not only financial losses but also the value of reputations and brand good will.

Innovation is a complementary approach. Because the greatest danger is posed by attacks that have never been seen before, they cannot be anticipated using traditional methods. Machine learning may offer a solution, scouring the network for suspicious activity and responding appropriately. Predictive analytics can help predict where hackers will go based on what steps they have already taken, blocking further penetration and minimizing disruption. This is not to suggest that humans will soon be replaced by machines. Recent research at MIT’s Computer Science and Artificial Intelligence Laboratory suggests that combining machine learning with the supervision of human security analysts may provide the most effective solution.

Cybersecurity measures are rapidly becoming more sophisticated, but asset managers are rarely on the leading edge of these advances. When asked whether their digital security efforts employed artificial intelligence or machine learning, only 13% responded affirmatively (Figure 15). Diversified firms are much more likely to use cutting edge technology than private equity firms.
The dearth of extensive planning or sophisticated countermeasures is understandable when spending is analyzed. Most firms allocate 10% or less of their overall IT budget to cybersecurity (Figure 16). In a few cases, this rises to more than 30%. Spending for most firms is likely to go up even further. Almost nine out of 10 diversified firms say they plan to increase spending on cybersecurity during 2017 (Figure 17).

Given where they are starting from and the traditional nature of the asset class, PE firms appear destined to lag other types of managers in the near term, but even half of all PE firms say that spending increases are in the works. This uptick in activity among PE firms is validated by other research that shows cybersecurity is likely to be a top IT cost driver in 2017, alongside initiatives to improve the investor experience, refresh legacy technology, and expand cloud computing. Indeed, according to PwC’s findings from their Global State of Information Security Survey 2017, 75% of respondents have “increased cybersecurity spending as a result of the digitalization of their business.”

FIGURE 15
Does your firm employ machine learning or artificial intelligence in its digital security efforts?

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Diversified</th>
<th>PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>13%</td>
<td>43%</td>
<td>100%</td>
</tr>
<tr>
<td>No</td>
<td>87%</td>
<td>57%</td>
<td></td>
</tr>
</tbody>
</table>

Note: Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.

FIGURE 16
What percentage of your total IT budget is spent on cybersecurity?

<table>
<thead>
<tr>
<th>Percentage Range</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% to 10%</td>
<td>82%</td>
</tr>
<tr>
<td>11% to 20%</td>
<td>11%</td>
</tr>
<tr>
<td>21% to 30%</td>
<td>4%</td>
</tr>
<tr>
<td>31% to 40%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Note: Totals may not add up to 100% due to rounding.
Source: 2016 SEI Cybersecurity Survey.

FIGURE 17
Do you plan to increase spending on cybersecurity in 2017?

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Diversified</th>
<th>PE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>57%</td>
<td>86%</td>
<td>50%</td>
</tr>
<tr>
<td>No</td>
<td>43%</td>
<td>14%</td>
<td>50%</td>
</tr>
</tbody>
</table>

Source: 2016 SEI Cybersecurity Survey.
IMPLICATIONS FOR ASSET MANAGERS

How can investment firms combat the cyberthreat most effectively? A good first step is to understand that it is not just an IT issue and that meaningful changes to corporate culture are likely to be necessary. Cybersecurity is also just one part of a holistic data protection plan. As operations become increasingly digitized, it becomes paramount that firms have the appropriate policies, procedures, checks, firewalls, and redundancies in place. Whether physical or digital, firms need to know where all of their data is being stored, processed, and transferred.

People are often the most vulnerable part of the equation, and devastating breaches originate with the compromising of virtually any employee. Anybody can be phished across myriad email and social network platforms, and once access is gained, the perpetrator has multiple options to disrupt operations or work out a way to get paid for his or her efforts.

This kind of problem cannot be solved by simply purchasing new technology or hiring a new employee. Responsibility and awareness should ideally span the entire enterprise, reflecting an integrated approach that includes all external connections. It helps to involve the board of directors in order to “set the tone” at the top of the organization.

It is important that everyone from the board down understands cybersecurity is an ongoing battle. There is no end game. There is a natural tendency to focus on the past, but emerging and future threats are ultimately more dangerous, so adaptability is critical. Existing technology can help identify and neutralize incoming threats, but newer technology is increasingly able to predict hacks and devise solutions to yet-as-unknown attacks.

Prevention, detection and recovery are equally vital. Preventative steps include things such as encryption, firewalls, permissions, backup and training. Much of this work is structural. Data need to be classified. Data that flow across internal and third-party infrastructure need to be mapped from creation to destruction, with all access points in between. Contractual obligations with service parties need to be reviewed and updated if necessary.

Not all prevention is necessarily expensive or even technology-based. Sometimes a simple procedural change can stymie major threats. A good example is the growing threat of fraudulent transfer requests from clients with hacked email addresses. Simply requiring telephone verification can greatly diminish this particular risk. Other simple preventative steps include using strong passwords, shredding sensitive documents, not opening suspicious emails, and keeping antivirus software up to date.

The fact that many attacks happen without managers even being aware of them accentuates the difficulty inherent in detecting cyberattacks. It can sometimes take months for a breach to be detected, but shortening that time can greatly reduce disruption and save money. Research has shown that firms that “complete a post-mortem within 30 days save an average of $1 million.”

Recovery is a multifaceted endeavor that requires the participation of multiple teams. Serious breaches in particular require the attention of an incidence response team who can focus on efficiently returning operations to normal and safeguarding assets from any further damage. They, in turn, will need to coordinate with a crisis communications firm to liaise with investors, employees and media. Outside counsel with cybersecurity expertise may need to be called upon as well.

Cybersecurity plans need to be documented in order to be effective, but the enforcement of policies is just as important. Proof that policies and procedures have been implemented offers protection not only from cyberattacks, but regulatory scrutiny as well.
One paradoxical aspect of cybersecurity that often gets overlooked is the fact that the customer (or investor) experience is often negatively affected by cybersecurity initiatives. By responding to cyberthreats, many firms have placed a greater burden on their clients, causing the quality of their experience to decline. It is tempting to see this—like TSA checkpoints at airports—as an inevitable consequence of heightened security. A more thoughtful approach is to segment clients and design a cybersecurity plan that delivers the desired client experience to those who prefer convenience, those who prefer security, and those who prefer a balanced approach.

Similarly, firms will want to prioritize their spending according to the value of the data in question. Sensitive data, such as social security numbers, or strategic assets, such as trading algorithms, for example, are likely to be high priorities protected by multiple layers of security. Other types of information may not demand a similar level of attention or budget.

Ultimately, a cybersecurity plan should take into account known and potential threats, regulatory requirements, the firm’s risk management strategy, due diligence requirements, and client preferences. It is a daunting task for many firms, but there is a wide array of help available. Consulting firms, technology vendors, and service providers bring specialized expertise. A growing body of knowledge makes it possible for anyone to bring themselves up to speed on the primary issues and solutions available. Cloud computing offers new delivery models for threat intelligence, while big data analytics promise to change what is even possible when it comes to security. Investment firms would be wise to leverage as many of these resources as possible in order to develop or upgrade their cybersecurity plan. As the cyberlandscape continues to evolve and threats multiply, cybersecurity plans have quickly gone from being good ideas to becoming indispensable assets.
ABOUT THE SURVEY

SEI surveyed 40 investment firms in late 2016 on the issue of digital security. Responses were collected from diversified asset management firms as well as PE firms. PE firms account for 73% of those responding to the survey, while diversified asset managers comprise the remaining 27% (Figure 18).

Just more than half of the firms taking part in the survey are based in the U.S. (Figure 19). Firms from the U.K. and Europe account for another 21%, while Asian firms as well as those from other parts of the world account for the remainder.

A number of data points have been tabulated according to the size of the responding firm. For the purposes of this paper, smaller firms are defined as those with less than $1 billion of assets under management (AUM), while larger firms are defined as those with more than $1 billion of AUM. The former make up 56% of the total, while the latter comprise the remaining 44% (Figure 20).
ABOUT SEI

SEI (NASDAQ:SEIC) is a leading global provider of investment processing, investment management, and investment operations solutions that help corporations, financial institutions, financial advisors, and ultra-high-net-worth families create and manage wealth. As of March 31, 2017, through its subsidiaries and partnerships in which the company has a significant interest, SEI manages or administers $779 billion in hedge, private equity, mutual fund and pooled or separately managed assets, including $297 billion in assets under management and $478 billion in client assets under administration. For more information, visit seic.com.

ABOUT SEI’S INVESTMENT MANAGER SERVICES DIVISION

Investment Manager Services supplies investment organizations of all types with advanced operating infrastructure they must have to evolve and compete in a landscape of escalating business challenges. SEI’s award-winning global operating platform provides asset managers with customized and integrated capabilities across a wide range of investment vehicles, strategies and jurisdictions. Our services enable investment managers to gain scale and efficiency, keep pace with marketplace demands, and run their businesses more strategically. SEI presently partners with more than 300 traditional, alternative and sovereign wealth managers representing over $15.5 trillion in assets, including 35 of the top 100 managers worldwide. For more information, visit seic.com/ims.

SEI KNOWLEDGE PARTNERSHIP

The SEI Knowledge Partnership is an ongoing source of action-oriented business intelligence and guidance for SEI’s investment manager clients. It helps clients understand the issues that will shape future business conditions, keep abreast of changing best practices and develop more competitive business strategies. The SEI Knowledge Partnership is a service of the Investment Manager Services division, an internal business unit of SEI Investments Company.

CONNECT WITH US

Twitter: @SEI_KP
LinkedIn: SEI Investment Manager Services
SOURCES

2 2015 Cost of Cyber Crime Study, Ponemon Institute, August 2015.
3 “AI and cybersecurity will be more important than ever in 2017,” Hira Saeed, VentureBeat, December 27, 2016.
6 “Cyber: Think risk, not IT,” PwC, April 2015.
14 2015 Cost of Cyber Crime Study, Ponemon Institute, August 2015.
The Investment Manager Services division is an internal business unit of SEI Investments Company. This information is provided for education purposes only and is not intended to provide legal or investment advice. SEI does not claim responsibility for the accuracy or reliability of the data provided. Information provided by SEI Global Services, Inc.