KPMG
cutting through complexity

Nine recommendations for alternative funds battling cyber crime

kpmg.com

Cyber criminals steal user names and passwords and use it to conduct financial trading activity illicitly.

Hackers seek ransom payments for private information of a prominent investor.

Your fund headlines the paper when an attack crashes your trading network and disrupts the financial markets.

> The growing threat level, the changing technology landscape, and increased compliance pressure have created a perfect storm of cyber risk.
>
> – Glenn A. Siriano,
> Principal, Information Protection

A recent New York Times article says cyber criminals are zeroing in on alternative investment (AI) funds, many of which oversee massive pools of assets but haven't invested sufficiently in security[i]. Furthermore, a report on the Operation Cleaver campaign indicates that financial services, alternative investment and private equity firms are targets for nation state actors[ii] . It's no wonder many fund managers feel as if they are in a losing battle against cyber crime.

KPMG explored cyber security in the AI industry during a January 2015 webcast featuring our own cyber security specialists. During the event, we polled approximately 2,000 AI managers about their experiences with cyber crime. This article shares the findings and provides AI managers tips for minimizing cyber risk.

i Cybercriminals Zero In on a Lucrative New Target: Hedge Funds (The New York Times, 6.19.2014)

ii Operation Cleaver Report (Cylance, 2014)

The front lines

Here's what fund managers face on the front lines of today's cyber security conflict.

The enemy has evolved

Today's hackers include organized crime syndicates, stealing intellectual property and personal information from corporate networks. These assets are a goldmine to the cyber criminals, who profit directly, seek ransom payments or sell on the black market.

Or, they are foreign nation states, intent on disabling the U.S. economy or destroying reputations through embarrassing and costly intrusions.

And while recent coverage revolved around payment card industry (PCI) data, advanced persistent threat (APT) actors are now going after intellectual property, merger and acquisition data, personally identifiable information (PII), and any other data that might give an attacker applying APT techniques a leg up.

The battleground has expanded

Organizations today need to protect a widening perimeter that includes third parties, with their own ecosystem of software, systems, desktops, laptops, and mobile devices.

And complicating matters further, smart and wireless technology, like printers, may connect to your core IT infrastructure and could be the weak spot cyber criminals exploit.

The cause is more important than ever

Our intelligence tells us that cyber attacks are going to become more frequent, more sophisticated and more dangerous as time goes on.

Just look at how losses are mounting. KPMG's 2013 Data Loss Barometer Survey found that the average loss by a U.S. financial services company from cyber breaches was $23.6 million[iii] , while a 2014 Ponemon Institute study found the cost of a data breach across industries was $3.5 million, 15 percent more than the prior year[iv].

Spend is skyrocketing, too. Gartner estimates that the overall worldwide security spend on technology and services will reach $76.9 billion in 2015[v]. But will this spend be effectively directed?

iii Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis (Ponemon Institute, 5.5.2014)

iv Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware (Gartner, 8.22.2014)

v Research conducted through a survey of approximately 2000 alternative investment managers during a January 2015 KPMG webcast

Nine cyber defense recommendations

AI funds need to step up their defenses to avoid the reputational and financial damage of a major cyber breach. From our extensive work advising funds on best practices across the cyber security spectrum, here are nine strategies to help funds battle cyber crime.

1 Rethink the governance model.

Cyber security is a business problem, not just an IT problem. It should be treated as such and handled as such. A recent KPMG poll encouragingly found most funds (82 percent) have a dedicated information security officer, but all "C" level executives must be engaged in the prevention and response to an attack.

2 Manage the internal threat.

As the universe of people with access to your IT infrastructure explodes, funds need to take internal security seriously, especially those with Bring Your Own Device (BYOD) programs, online operations, or applications in the cloud. Disgruntled employees, contract employers with privileged access, and fraudsters could all pose a risk.

3 Build a cyber awareness program.

People are the weakest link. As such, employee training and development should be a core aspect of any fund's security program, and firms should validate training through targeted social engineering. Effective user awareness is also critical for any external providers handling your data, which leads to our fourth strategy.

> Our intelligence tells us that cyber attacks are going to become more frequent, more sophisticated and more dangerous.
>
> – Kevin M. Goldstein, Director, Management Consulting

Improve third party security assessment.

Third parties could expose funds to cyber risk. Major retailers, for example, have been compromised through their heating, ventilating and air conditioning (HVAC) vendors[vi]. Our poll shows that only 44 percent of funds are focused on third party data security oversight. As your third party network grows, look closely at what type of sensitive information you share, how it is encrypted, how vendors secure it, and how your organization can reclaim previously provided data.

Consider emerging technology risks.

Closely review the security implications of moving to the cloud or sharing information on social media. Install security software on devices. And, like 64 percent of funds in our poll, block the ability to download or remove certain sensitive information. Given the dangers of advanced persistent threats, strong network protection and safety measures are especially important today.

Enhance security intelligence.

Beyond installing the latest patches and managing firewalls, funds can step up security intelligence by collaborating with security intelligence aggregators, analyzing log data, and introducing new models for identity, trust, authentication and entitlements.

Develop an incident response plan.

Unlike the majority of the funds we surveyed, you should have a formal cyber security incident response plan you follow in the event of a network compromise. And you should regularly test the plan, just like any other business continuity program. The plan should have both executive and technical components and identify all participants in your response, as your customers will expect to hear from business executives should an incident occur.

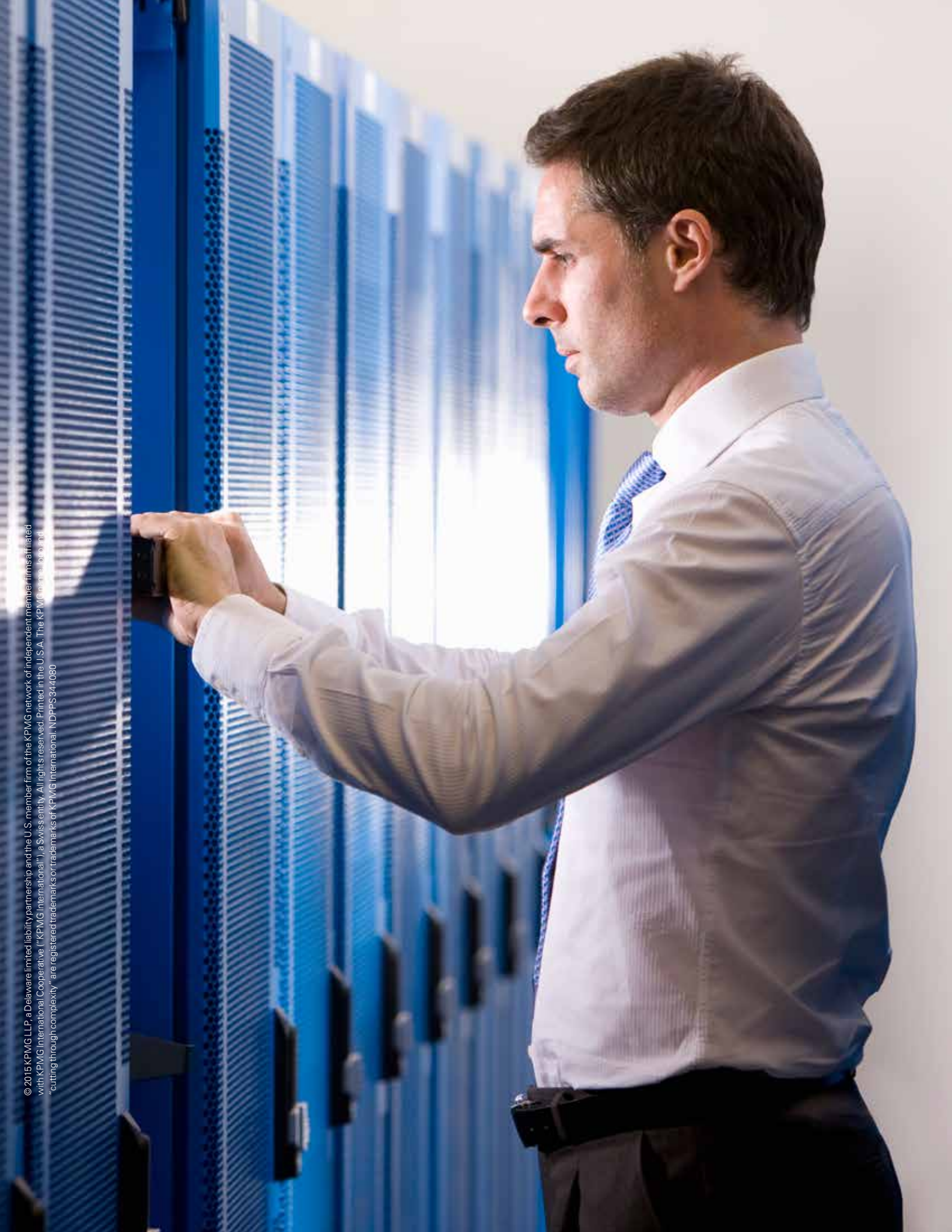
Conduct a risk assessment.

The assessment can help you understand your cyber risk, including how you rank against peers and against industry standards, so you can focus resources on improving the most vulnerable areas that represent the highest areas risk to your business. The risk assessment should also include a prioritized action plan for strategic security initiatives.

Enhance data classification and management.

Do you know what your most valuable data is, where it resides, how many copies exist, or even who owns it, let alone who is entitled to view it? A data classification program, which involves categorizing data according to its sensitivity, is an extremely important step in building a secure organization. To build a risk-based security controls program, funds should carefully consider how they define their levels of data. What's more, you can no longer collect unimaginable volumes of data without consequence. Safeguarding it also requires a robust data privacy and security strategy..

vi HVAC Vendor Eyed as Entry Point for Target Breach (CNN Money, 2.6.2014)



Feel more secure about Cyber Security.
Contact KPMG.

Glenn A. Siriano
Principal – Information Protection and Business Resiliency
KPMG LLP
Stamford Square
3001 Summer Street
Stamford, CT 06905-4317
T: +1 203-406-8242
E: gsiriano@kpmg.com

Greg Bell
Principal – Information Protection and Business Resiliency
KPMG LLP
300 Peachtree Street, NE
Suite 2000 Atlanta, GA 30308
T: +1 404-222-7197
E: rgregbell@kpmg.com

Tony Buffomante
Principal – Information Protection and Business Resiliency
KPMG LLP
303 East Wacker Drive
Chicago, IL 60601
T: +1 312-665-1748
E: abuffomante@kpmg.com

Kevin M. Goldstein
Director – Management Consulting Alternative Investments Advisory
345 Park Ave
New York, NY 10154
T: 917 438 3850
E: kevingoldstein@kpmg.com

kpmg.com