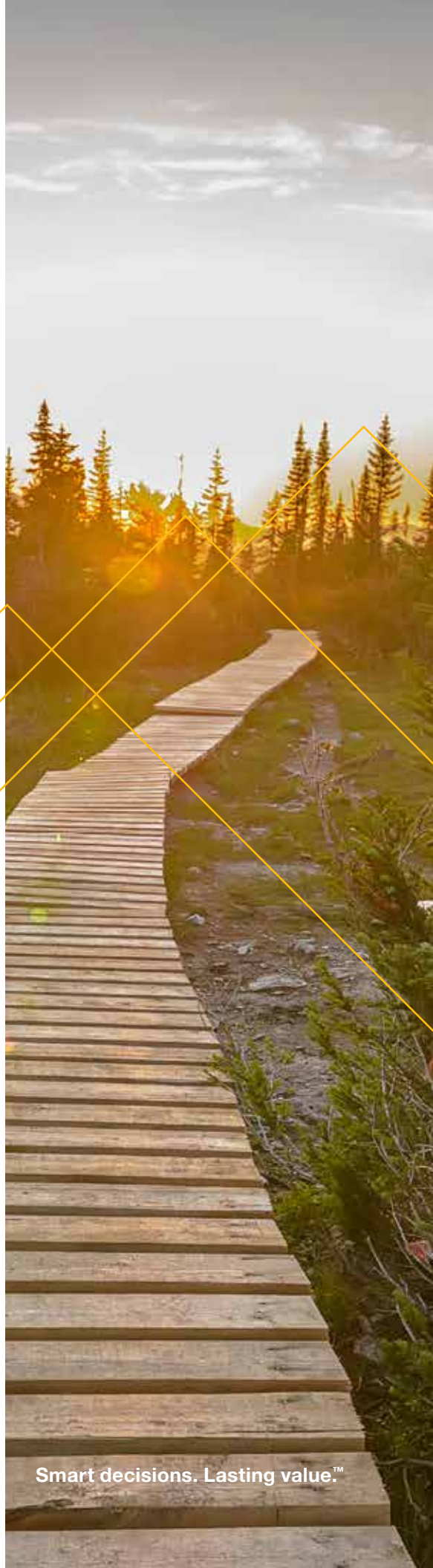
Crowe

Risk Assessment and
Response Case Study

Preventing Losses From Cyberattacks

IT Security Services for Private Equity Groups



Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.℠

Among companies large and small, the threats of cyberattacks are rising and no longer are confined to retail and financial services businesses. Tactics for intrusion, enabled by automation and machine learning, evolve continually and produce increasingly sophisticated methods of disruption.

For businesses, intrusions can result in substantial time and resources spent on recovery efforts, legal issues, and responding to regulatory enforcement action. Depending on the scope, financial losses, and extent of data compromised, the negative publicity and reputational damage can drag down a company's value for weeks, months, or years.

Well-informed investors are skeptical about investing large sums of money with businesses having lax controls over IT security. Consequently, private equity groups, as well as conglomerates with diverse holdings, are focusing on assessing and reducing cyberrisk in multiple businesses, industries, and geographies – an ongoing responsibility, given that cyber intrusion tactics are always changing.

The Need for Thorough Assessments

Crowe has been helping its private equity clients by providing due-diligence services related to IT, developing IT strategy road maps and assessing and managing IT risks – all of which help our clients make smart decisions that help create lasting value. What follows is just one example of what we have done to help clients fend off cyberthreats.

In this case and starting in 2015, one private equity client asked Crowe to help with a broad assessment of cyberrisks across its portfolio of businesses. A successful phishing scheme had been detected at one company, and the private equity group wanted to evaluate security and avert further attacks on other holdings.

To recommend smarter ways of managing cyberrisk on an ongoing basis, the Crowe project team outlined a two-phased, risk-based approach to accelerate a comprehensive review of the client's portfolio. The first phase focused on assessing inherent risk in each company, and the second on testing the effectiveness of controls and attack responses to determine residual risk. The project would conclude with recommendations for quick fixes, as well as long-term strategies, to bolster IT security across all holdings.

Phase One: Assessing Inherent Risk Across Holdings

The Crowe project team looked at holdings across industrial sectors, conducted research, and developed a questionnaire to determine which companies had the most assets to protect. The team looked to see how risk varied by organizational size, asset types, as well as by level of IT security experience possessed in each company.

The survey sought answers to general questions about each company (e.g., size, industry, and organizational structure) and more specifically about:

- Types of data (e.g., credit card, health-related, and trade secrets) collected and stored
- Size of the IT department
- Resources, if any, dedicated to IT security
- Knowledge of cyber intrusions
- Insurance against cyberattacks

A survey link was sent to a list of specific senior managers at each company, leading them to a secure Crowe platform to take the survey. Some questions had radio buttons and drop-down options to click on, while others were structured to be open-ended – thereby enabling respondents to offer explanations or ask questions.

If a respondent did not feel competent to discuss certain areas of the organization, the survey allowed for input from multiple managers or directors to obtain a more accurate picture of risk and control structures.

While analyzing the responses, the Crowe project team paid greater attention to answers to three questions:

1. How many people do you have dedicated solely to information security?
2. Do you perform vulnerability assessments and penetration testing regularly?
3. What kinds of data are being collected and stored?

From previous experience, the project team knew answers to these questions would reveal more about inherent risk than, for example, risk within the client's industry. Consequently, responses to these questions received more weight in the scoring and had more influence on overall rankings.

Based on strategic information (e.g., the percentage of ownership or the investment strategy for each holding), leaders of the private equity group made some adjustments to the prioritized list Crowe presented at the conclusion of phase one. The collaboration between the client's leaders and the Crowe project team helped set a firm direction for holdings perceived as highest priority for inspection in phase two.

Phase Two: Testing Cybersecurity Response in High-Risk Holdings

Companies perceived to be at higher risk were grouped in four waves, and the project team has now moved forward with the first wave of six companies for closer inspection. The project team has given senior managers in each of these businesses a list of requested documents including information security policies, IT operational procedures, and disaster recovery plans. In addition, the project team is following up with unanswered questions about issues identified from prior survey responses.

Phase two also includes a detailed testing assessment that includes both internal and external scans of network and system security. In common terms, this step has Crowe security "good guys" trying to find weak spots before the "bad guys" exploit the vulnerabilities.

Each company participating in phase two receives a remote security appliance – an economical way of assessing IT security. The device can be plugged into each network, and the testing exercises detect gaps between policies and procedures to evaluate the actual effectiveness of defense tactics.

Findings from this phase reveal residual risk. While a company might have high inherent risk, for example, due to massive volumes of credit card, personal, and healthcare data, its IT security team and automated defenses might be highly vigilant and effective, thereby reducing residual risk to an acceptable level. In contrast, another company might have medium inherent risk, but, when coupled with unpatched servers, weak password policies, and an internal network design that is too easy to hack, the result could be high residual risk.

By grouping companies for deep inspection in phase two, Crowe is able to keep costs down. Travel costs are reduced, and multiple phase two evaluations can be conducted simultaneously due to the efficient use of:

- Remote security appliances, also known as "black boxes," distributed to companies throughout the world
- A lean cybersecurity team operating under a single project manager and conducting examinations at several companies during the same two-week period
- Project structure, with six to seven companies grouped in each wave, for deeper examination
- Frequent communication to identify trends and observations across the portfolio

Phase two is expected to produce "quick win" recommendations that will be relatively easy to implement in six months or less. Crowe will also issue strategic recommendations of paths the parent company can take in the next two to three years to develop a stronger security posture across holdings.

Cyberthreats Grow in Sophistication

The nature of cyberthreats doesn't remain the same for very long. Spear-phishing attacks, for example, were relatively common in 2015, but after companies increased their awareness and defenses, cyber criminals in 2016 turned to new schemes, including ransomware – in which IT systems were effectively "frozen" until the demanded bounty was surrendered.

What type of attacks will emerge in 2017 or 2018?

Hackers located throughout the world share automated tools to facilitate attacks. Consequently, it is vital for companies to remain curious about how methods of intrusion are evolving and reassess the effectiveness of cybersecurity programs.

The risks are particularly high for private equity groups because of their diverse holdings. The risks can vary by company size, types of assets held, and security defenses. Only through constant vigilance can companies sustain a strong defense and minimize the reputational risks and financial damages resulting from cyberattacks.

In the face of these ongoing threats, we stand ready to assist our clients as needed.

About Crowe Private Equity

Crowe is one of the largest public accounting, consulting, and technology firms in the United States. From transactions to portfolio and fund solutions, Crowe offers a comprehensive suite of services to help private equity (PE) firms maximize value. Our strong reputation in private equity and many industries is built on extensive qualifications including:

- A private equity client base with a combined total fund size of nearly $200 billion
- More than half of our top 50 clients are PE groups
- Senior-level involvement throughout the deal life cycle
- A national and international network for access to local, on-the-ground expertise
- A hands-on approach with one relationship manager for each PE firm

Connect With Us

For more information on Crowe risk consulting services, please contact:

Christopher Wilkinson
Partner, Risk Consulting Services
Crowe
+1 312 899 8405
christopher.wilkinson@crowe.com

Kiel Murray
Technology Risk Services
Crowe
+1 214 777 5241
kiel.murray@crowe.com

crowe.com

PEG-17000-032A