

Corporate Security

More Than a Lock on the Door

As the global economic crisis persists, businesses and organizations are looking to protect their most valuable assets. Some companies will shore up client relationships or protect revenue streams against market decline. Most will seek to cut costs, investing less in areas that are least required to remain solvent and competitive. Unfortunately, many leaders take measures to "secure the future of their business" while overlooking security itself. They do so at great risk; security threats are financial threats.

by R. Jason Straight

"Corporate security" conjures images of thick steel doors, uniformed guards, and closed-circuit television. However, it must also encompass mitigation of personnel risks, information security, and intellectual property protection.

Personnel risks

In the economic downturn, motives for employee misconduct are on the rise. Increased potential for low morale and high tension surrounding layoffs combined with personal economic pressures on employees create unanticipated personnel risks for companies.



These risks can be mitigated through employee background screening, a universal best practice for corporate security. Given the high proportion of incidents that originate from within organizations – from workplace violence to data theft – it is essential to run checks on potential employees, vendors, and contract personnel. An informed hiring manager is in a better position to make good decisions about whom to trust with the company’s assets and reputation. However, only 44% of companies globally conduct regular employee screening, according to the Kroll Global Fraud Report 2009/2010.

Pre-employment background screening needs vary both by industry and by the employee’s position. A credit check is likely unnecessary for an employee who will not be acting in a financial role, but companies will find it valuable to perform criminal record checks on all new employees. Employment and academic verifications can be an important tool for ensuring that an applicant has the appropriate credentials. Résumé fraud may not indicate that the individual is a security threat, but it is a warning sign for possible future misconduct.

Information security

History shows us that virtually every technological advance can be misused. In the world of digital information, the abusers become the hackers, cyber terrorists, and data thieves reported in the media. Information technology has become an increasingly important front to defend, especially in light of the fact that more than 90% of business information is held in a digital format and approximately 70% of that data is never printed on paper. This information includes everything from sensitive documents and proprietary plans to customer records and employee data. For companies that store personal information about customers or employees, the economic and reputational losses resulting from a data breach can be severe.

Cyber security

Most often, information security incidents originate within an organization. According to a 2006 Ponemon Institute survey, 78% of information technology professionals in the United States said their companies have suffered unreported insider-related security breaches. To avoid information leakage, organizations should create and enforce a policy governing the use of their information assets. This can include rules relating to employee use of e-mail, websites, media sharing sites, social networking, and instant messaging. But simply having a policy in place does not guarantee success, especially if employees are unaware or untrained.

An employee traveling with an encrypted laptop might assume that the corporate data on that computer is secure. However, Kroll was recently engaged for a computer forensics assignment in which a laptop had been stolen while it was in “sleep mode.” We found that the system only invoked absolute protection when the computer was turned off completely. We have also seen cases in which an attacker drops USB data keys in the company’s parking lot: If an employee inserts one into their computer, the software on the key can infect the machine with malware that can be used as the basis for attacking the company’s network and stored data.

Essential cyber security prevention measures must be supplemented with detection tools and response plans. On the network level, this might involve setting up a Security Operations Center (SOC) or installing network sensors that can collect the data needed to identify threats to the network and communicate them to a monitoring center where specialists can look for problems on a 24/7 basis. In crisis situations requiring immediate assessment of cyber-security preparedness, experts can deploy a “Rapid Deployment Network Sensor Array and Monitoring Package,” otherwise referred to as a “SOC in a Box.”



Data breach and identity theft

Businesses and other organizations that collect and store personal information face special security risks. The total average costs of a data breach grew to \$202 per record compromised, an increase of 2.5% since 2007 and 11% compared to 2006, according to a 2008 survey by the Ponemon Institute. Direct costs incurred by a company alone averaged \$6.6 million per incident in 2008, up from \$6.3 million in 2007 and \$4.7 million in 2006.

Government regulation of data breaches is also increasing. Organizations are facing new laws and regulations that increase their responsibility to protect data, investigate incidents, and take steps to retrieve lost data. The Federal Trade Commission's new "Red Flags Rule" requires many organizations to develop and implement formal, written, and revisable identity theft prevention programs. In general, the consequences of noncompliance can be severe, potentially resulting in financial penalties, reduced stock value, victim or shareholder litigation, loss of customer confidence, and lost sales revenue.

The problem requires a multi-dimensional solution. Both high-tech and low-tech identity theft attacks hinge on corporate vulnerabilities that facilitate the pilfering of sensitive customer data. Attacks can often be thwarted with the right preventative measures. Among them:

- Keeping software current with security updates.
- Knowing where important customer data resides.
- Collecting evidence when an incident occurs.
- Recognizing the risks of wireless data transmission.

In the event of a data breach, it is important to quickly understand what, why, and how it happened. Security problems will likely need to be remediated, and forensic analysis will be necessary to quantify the scope of the breach. Individuals whose personal information has been compromised must be notified, which can be a challenge as legal requirements vary on a state-by-state basis.

Intellectual property

Intellectual property (IP) is another intangible asset to be managed and protected. Recent studies have shown that intangible assets represent more than 70% of the value of a typical U.S. company's total assets. Given the high-value and highly portable nature of IP, it is under increasing threat, especially as companies reduce staff in the wake of market turmoil. Employees who feel aggrieved may decide to leave with the company's trade secrets, customer lists, pricing, or other sensitive data. In one instance, a foreign competitor hired a critical group of engineers away from a rival firm. Within a few months, the competitor filed a patent on technology that had taken its rival years to develop. The senior management of the rival firm was not even aware that its employees had defected to the foreign competitor until it was too late.

IP protection requires attention to both information technology and physical security. The risk of a hacker intercepting e-mails containing blueprints or design specifications is no greater than that of a double-dealing employee walking out the door with a prototype to be reverse engineered by a competitor. It is critical to take proactive IP protection steps:

- Conduct an IP audit.
- Design enforceable IP rights.

- Know your local partners, wherever they are.
- Know your supply and manufacturing chain.

The overarching goal should be to establish a culture of IP protection within an organization. Companies taking the above steps not only guard IP better, but also send a clear message about the high value they place on intellectual property.

Physical security

Corporate security budgets balloon in boom times or, more often, in response to an increase in perception of threat. However, in the wake of the global economic crisis, we have seen physical security budgets shrink. Risks continue to evolve, and the tactics of those who seek to do harm will always adapt to changing security postures. All physical security plans require regular audit, testing, and review to ensure that procedures, systems, and training are current.

Integrated design and concentric circles of protection

While integrated design for site perimeters is already common practice for government and high security applications, companies increasingly opt for this more comprehensive approach in new construction. Integrated design combines the architectural features of Crime Prevention Through Environmental Design (CPTED) with traditional technical, physical, and operational security elements. The most effective application of CPTED concepts results in architectural features that are barely recognizable as perimeter defense, but instead are presented as well-planned architectural designs. Perimeter security often takes a layered approach, establishing a set of concentric circles. With this layered approach, organizations can control access to their environment



further out, ensure that undesirables have several hurdles to breach before reaching critical areas, and gain crucial time to respond to the threat.

Conclusion

Security risks do not sleep through difficult economic times. Awareness and in-depth defense are critical, and by taking a broad view of the different elements of corporate security companies are able to make better decisions to protect their facilities, employees, data, and intangible assets.



R. Jason Straight, Esq. is a New York-based senior managing director of Kroll. He manages a team of experts specializing in computer forensics, network intrusion, data breach investigations, litigation readiness consulting, and e-discovery response services. Mr. Straight can be reached at jstraight@krollontrack.com.

Mr. Straight's Kroll colleagues Jenifer DeLoach, Alan Brill, Brian Lapidus, Nick Blank, and Ray Blackwell contributed to this article.