SPECIAL REPORT: Healthcare, Higher Education, Finance Industry Clients Top Three Cyber Targets in 2013

AS A GLOBAL LEADER in cyber investigations and incident response, Kroll aided a record number of clients with data breaches of all severities in 2013. Looking ahead to what organizations might expect in 2014, we examined data from cases we handled for U.S. clients in the past year and discovered trends with major implications for all industries, and in particular healthcare and higher education. This report highlights our findings and the forces we see driving those results.

Healthcare at greater risk from insiders; higher education faces more malicious attacks

Three industries accounted for nearly two-thirds of all client events: healthcare (38%), educational institutions (13%) and financial institutions (9%). A closer review of the data shows that healthcare and higher education differ dramatically in the cyber risks confronting them.

Our 2013 cases show that approximately 78% of healthcare cyber crises were tied to human error and 22% involved an act of malicious intent. By contrast, over 73% of cyber events in the higher education market were traced back to a malicious act.

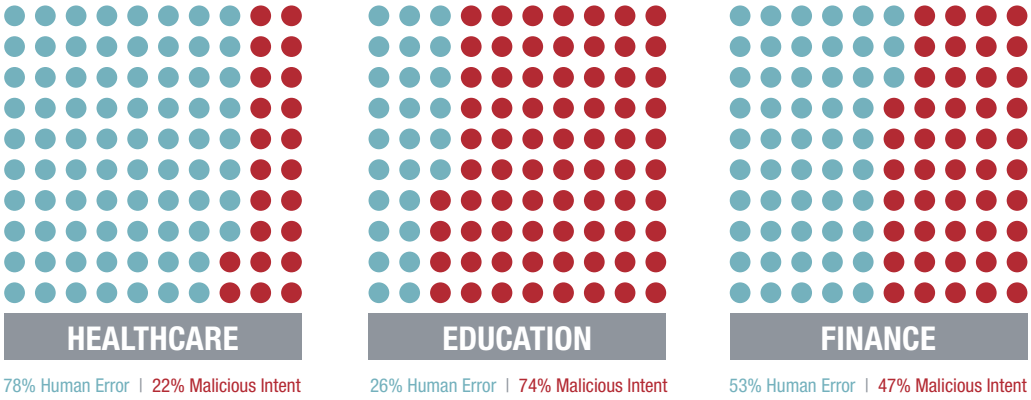
Are criminals more drawn to stealing data from educational institutions?

Educational institutions pose unique challenges from a security perspective. Educational institutions are populated with innovative, technically adept users within cultures that promote adaptation and change. The collaborative, open nature of most institutions makes the implementation of security protocols a challenge. In addition, while both sectors are regulated by federal privacy laws, the Health Insurance Portability

2013 KROLL CLIENT DATA BREACHES BY INDUSTRY*

38%	Healthcare	6%	Retail	3%	Technology	1%	Apparel	1%	Entertainment
13%	Education	5%	Consulting	1%	Food & Beverage	1%	Chemicals	1%	Transportation
10%	Other	3%	Insurance	1%	Manufacturing	1%	Energy		
9%	Finance	3%	Legal	1%	Not for Profit	1%	Engineering		

* Source: Kroll 2013 case study analysis from U.S. based clients.



THE INSIDER THREAT BY INDUSTRY

and Accountability Act (HIPAA) HITECH requirements have provided healthcare organizations with incentives to update security through oversight from the Department of Health and Human Services and Office for Civil Rights. Consequently, we have seen entities in this sector tightening their security protocols. Without similar regulatory development, educational institutions have not seen similar hardening of security walls and protocols.

Education and healthcare are also both rich sources of personal and financial data. Kroll's experience shows that more healthcare losses stem from improper controls over data and a lack of understanding of who has access to key data. Too often, data is kept unnecessarily, and too many people have access to it. As a result, simple human error can pose a greater risk to data loss.

As criminal activities continue to evolve—and as the current trend continues—educational institutions will sustain more numerous and persistent attacks in the near future. According to data from Privacy Rights.org, more than 114 higher education breaches have been reported in the past two years, exposing some 2.2 million records.

Recognizing prevalence, magnitude of insider threat a major step toward combating it

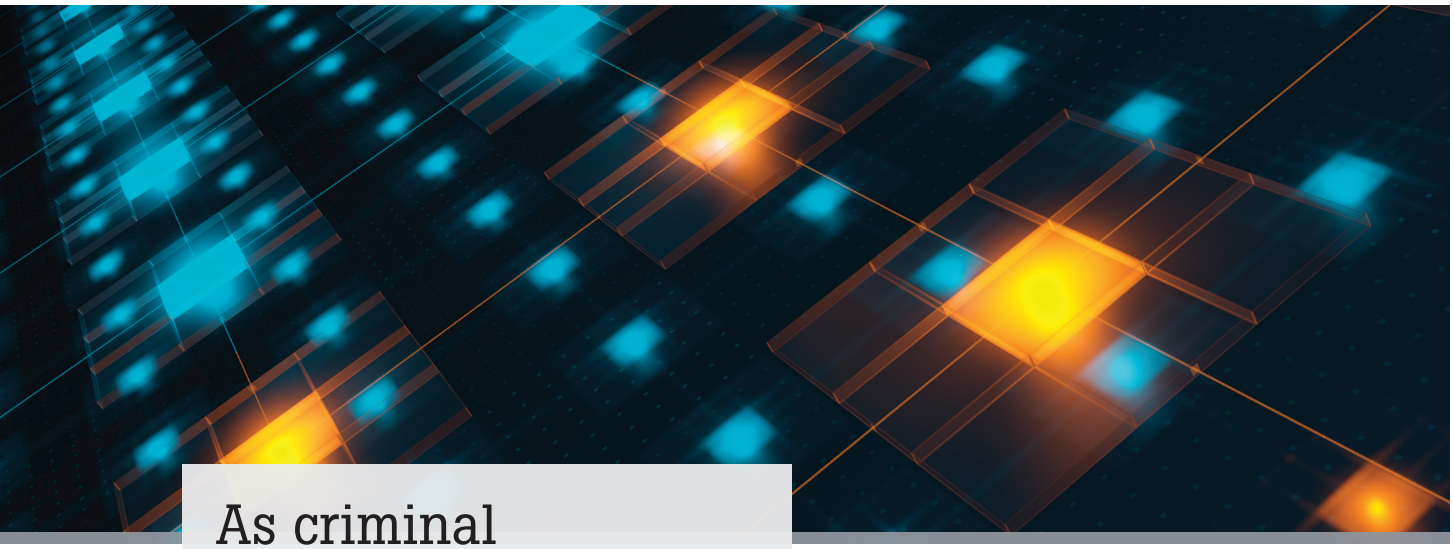
In Kroll's analysis of client cyber cases across all industries, 51% of breaches were tied to insiders. And we're not talking solely about malicious people with a company ax to grind, although they are part of the problem. Employees with the best of intentions are still careless; data is mishandled and files are disposed of improperly. As this activity continues unabated year after year, we anticipate that a significant number of data breaches will come at the hands of people on the inside in 2014.

People tend to discount the insider threat because it doesn't make the news. In its place, we see headlines about external credit card breaches and theft of personally identifiable information because regulations mandate accountability and punishment is expensive. Data breach is a self-reported crime, albeit one driven by regulation in certain instances. However, until real inroads are made towards training, with teeth and repercussions for lapses in protocol, people who "slip up" on data security at the office will largely go on operating under the risk radar. Changes are on the horizon, however, that will increasingly pull the curtain aside and reveal the insider who is often at the heart of a cyber loss.

As the federal government and individual states strengthen privacy breach notification laws and regulators implement enforcement efforts, the hidden nature of insider attacks will become more widely known—and with it, greater awareness of the damage that insiders cause. It is an insidious and complex threat. Thwarting the insider threat requires collaboration by general counsel, information security, and human resources. Organizations are going to need to spend significant resources addressing this challenging problem in 2014.

Vast majority of identity thefts undiscovered with credit monitoring

In the past, credit monitoring was the predictable solution for organizations that have experienced a breach. However,



As criminal activities continue to evolve—and as the current trend continues—educational institutions will sustain more numerous and persistent attacks in the near future.

according to a 2012 Federal Trade Commission (FTC) report, 88.7% of cases of identity theft would not have been found via credit monitoring alone. Effective January 1, 2014, the definition of "Personal Information" in California's state breach notification law was expanded to include "a user name or email address, in combination with a password or security question and answer that would permit access to an online account." As definitions and regulations are recast in the light of what consumers decide is personal and worth protecting, our clients must be able to provide meaningful solutions to the individuals affected by a data breach. Taking a more risk-based approach when determining what remedy to offer is a significant change from what we have seen in the past.

Pre-planning sets stage for an effective response with comprehensive, cost-effective resources

Data security and incident response have become high priorities for our clients. They are increasingly planning their approach to handling a potential cyber event—from asking for guidance on creating breach response policies and protocols to a full range of readiness activities, such as self-risk assessments, tabletop preparedness exercises, and vulnerability scanning.

This in turn has changed how they select a response partner. In the past, there was a tendency to go with the lowest cost provider. Today, organizations are asking partners about credentials and getting a detailed understanding of all of their capabilities prior to agreeing to use them in a data loss event. This pre-planning is helping organizations prepare and saving them significant costs as they negotiate rates before an event occurs.

Conclusion

Our 24-7 work culture and the liberation of data and devices via bring your own device (BYOD) and cloud solutions have created new security and human resource risks. Too often, organizations across all industries protect from the outside attack, but fail to address the risk of negligent and malicious insiders. It is simply not enough to test systems—effective data security requires all aspects of an entity to work together. Make sure that you are properly addressing these risks in a manner that complements your work flow, yet balances the risks and the costs.

Kroll can help

More than ever, Kroll is being approached by clients before an event occurs to ensure they are ready if and when they experience a loss. Kroll can help your team understand how your data can be at risk within your own institution and guide your planning, providing both technical and human-based solutions to manage risk. For maximum flexibility, you can take advantage of our many offerings in either standalone form or as an end-to-end, one-source solution. To contact a Kroll expert by region or specialty, read about notable cases, or download one of our latest reports, visit us at www.krollcybersecurity.com.

Brian Lapidus, Managing Director,
Identity Theft and Breach Notification Practice Leader, Kroll
Jonathan Fairtlough, Managing Director, Kroll

CONTACT

For more information, call or visit us online:
+1 866.419.2052

kroll.com

Kroll

THT-046 ITDB US – TRENDS