



**The Cyber Espionage Threat –
Implications for Corporate
Boards of Directors**

White Paper

Carl Young, Managing Director &
Chief Security Officer

October 26, 2011

STROZ FRIEDBERG

No company is immune to the threat of corporate espionage, and specifically to information loss or misuse via cybercrime. Unfortunately, there are many examples of the effects of cyber threats. Some of these have irreparably harmed corporate reputations and greatly affected their bottom line. For this reason, corporate espionage and cybercrime are topics of increasing importance to corporate boards of directors.

In view of increasing information security risks in corporate settings, Stroz Friedberg LLC, a leading global information security and digital governance firm, hosted a panel discussion on October 4 in Washington D.C. The discussion was led by [Senator Judd Gregg](#), and the panel addressed historical methods and origins of attack, as well as the viability of risk mitigation measures.

The discussion yielded useful insights on these issues that derive from both public and private sector experience. Panelists included [Shawn Henry](#), Executive Assistant Director of the Criminal, Cyber, Response and Services Branch of the FBI, [Mark Sopp](#), CFO and EVP of Science Applications International Corporation (SAIC), [Edward Stroz](#), founder and Co-President of Stroz Friedberg and [Carl Young](#), Managing Director and Chief Security Officer at Stroz Friedberg.

The panelists and ensuing discussion also generated comments from the audience to develop a broad consensus on corporate approaches to cyber security. In particular, panelists and audience agreed that it is necessary for corporations to adopt a predictive and preventative information security posture in addition to developing a robust incident response capability with respect to data breaches.

[Corporate Impact and Preparedness](#)

Corporations are collectively losing billions of dollars each year due to data security breaches. These same corporations must prepare for cyber threats based on an expectation that they will inevitably be targeted sometime in the future. From a risk management perspective, it is important for a board of directors to understand the potential and long-term impact of a single data breach to the corporate bottom line relative to the overall costs of risk mitigation.

Despite the multitude of security options, developing and implementing an effective information security *strategy* is not straightforward. Such an approach requires a corporate solution that is practiced by all employees and mandated from the top down. Specific measures that are essential to developing an information security strategy include the following:

- **Enhance Security Risk Awareness:** a practical knowledge of information security risk is arguably the most important first step in addressing cyber crime. Many of the recent high-profile attacks occurred because an employee opened a harmful e-mail attachment and did not recognize tell-tale signs of risk in advance. A basic knowledge of risk should be shared as a matter of corporate policy and promulgated within a non-accusatory environment.
- **Create an Incident Response Team:** organizations should establish and train an incident response team in the event of a data breach. The team should include professionals from relevant departments including IT, legal and corporate communications.
- **Establish Data Breach Notification Procedures:** unambiguous procedures should be established that specify whom to notify in the event of a potential data breach. The

immediate preservation of assets is critical to both an effective response and the preservation of evidence. This response protocol must be simple so that all employees are able to follow the instructions.

Public-Private Collaboration

It is essential that corporations partner with the government to help mitigate the risk of cyber attacks. A very basic step that will immediately lead to a better understanding of risk is to share information on an ongoing basis. Although this is definitely happening, more can be done by corporations and the government to facilitate this process.

Most of the IT infrastructure is owned and operated by private corporations. A government agency may be the first to notice an attack but may not be able to investigate fully due to privacy regulations. Furthermore, an attack on an individual corporation may be part of a broader scheme. However, private entities cannot effectively investigate nor prosecute an alleged lawbreaker without government intervention.

It is therefore essential to build robust if confidential lines of communications between the public and private sectors. This must happen in order to recognize threat trends on a national and international scale as well as to assist corporations in understanding their risk profile relative to those threats.

The Cyber Security Future

Cyber attacks are continually evolving and effective countermeasures must do the same. Although no one can predict the future of electronic communication and associated threats with certainty, some technology-related and regulatory trends are more likely, based on historical risk and future demands on system performance.

To conclude the discussion, the panelists offered their perspectives on the future of cyber security. The following represent some of the key points in that exchange:

- **Regulation and Compliance:** House and Senate lawmakers are focused on developing cyber security legislation to respond to increasing cyber attacks against private corporations and government entities. It is also possible that the Security and Exchange Commission (SEC) will investigate aspects of corporate cyber security issues, as revelations of this kind could expose information that is important to investors.
- **Breach Insurance:** Cyber security insurance will become commonplace due to the rise of civil lawsuits and the increasing costs of data breaches. The current estimated cost of a data breach is \$214 per compromised record, and averages \$7.2 million per data breach event, according to the [Ponemon's 2011 U.S. Cost of a Data Breach Report](#).
- **Technical Trends:** most on-line security applications exclusively utilize passwords to authenticate users. Future modes of authentication will likely incorporate behavior-based methods and thereby leverage highly personal characteristics that would be more difficult to spoof.

Contacts: Ed Stroz, Co-President
(212) 981-6541
estroz@strozfriedberg.com

Carl Young, Managing Director & Chief Security Officer
(212) 766-6004
cyoung@strozfriedberg.com

About Stroz Friedberg, LLC

Stroz Friedberg is a leading global digital risk management and investigations firm. The company specializes in digital forensics, data breach and cybercrime response, electronic discovery, and business intelligence and investigations. Working at the crossroads of technology, law and behavioral science, Stroz Friedberg provides technical assistance and strategic advice to help manage the inherent risks and responsibilities of doing business in a digital era. Learn more about the firm's capabilities and experience at www.strozfriedberg.com.