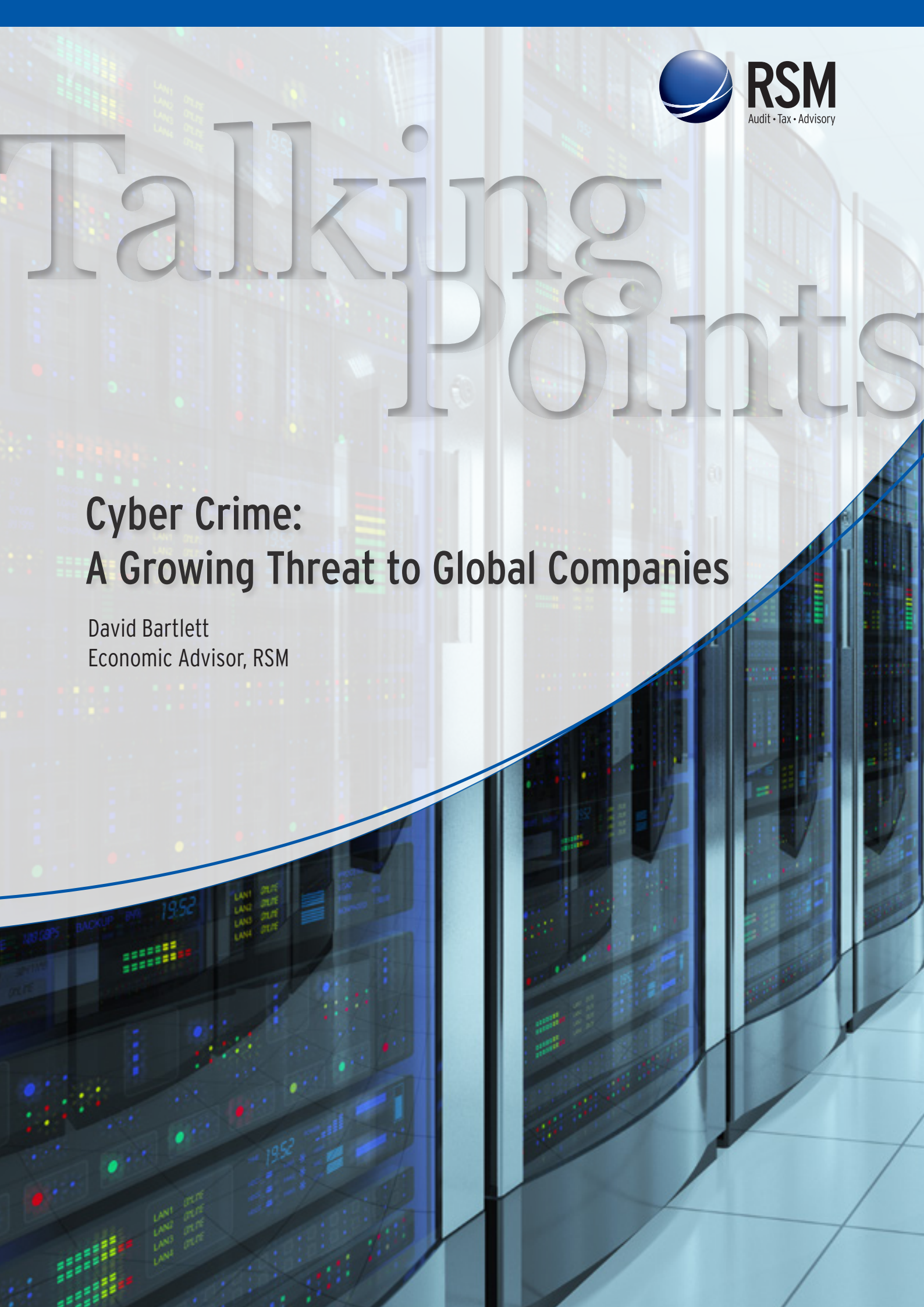
RSM
Audit • Tax • Advisory

Talking Points

Cyber Crime: A Growing Threat to Global Companies

David Bartlett
Economic Advisor, RSM



Introduction

Cyber security, once limited to the expertise of Information Technology specialists, has become a business-critical issue engaging senior corporate leaders worldwide.

A recent survey of corporate executives by Lloyd's of London ("Lloyd's Risk Index 2013") found that cyber crime ranked 3rd (behind high taxation and loss of customers) among the risks confronting global businesses. In a Lloyd's survey conducted just two years earlier, cyber crime ranked 12th in the list of risks facing business leaders–underscoring the sharp rise of cyber risk amid a rapidly changing technological and regulatory landscape.

During the RSM European conference in Bucharest, Yoav Tzruya, from JVP Cyber Labs, presented on cyber crime and the threats faced by businesses today. Among some of the greatest threats are: phishing, malicious software, disruption/defacing of the organisation, theft of financial information, and cyber attacks to steal intellectual property or sensitive data.

Many cyber attacks on businesses emanate from external agents: cyber criminal organisations (many based in Eastern Europe and the Former Soviet Union), "hactivists" (groups staging cyber attacks to advance political or ideological goals), and skilled individual hackers (exploiting the growing ease of penetration of internet systems). Cyber attacks have also become a geostrategic instrument of nation states, notably China and the Russian Federation - a phenomenon that has prompted NATO to include cyberspace as the fifth domain of war (joining land, sea, air, and space) in the organisation's Article V clause on collective defence.

But business leaders also cite malicious insiders as a growing source of cyber crime. A report by the risk management company Kroll ("2014 Cyber Security Forecast") indicates that nearly half of corporate data breaches stem from the actions of employees. The rising incidence of inside cyber attacks presents complex questions for IT, human resource, legal, and financial managers of affected companies.

Drivers of Cyber Crime

The growth of cyber crime results from the following factors:

- The global diffusion of the internet, which has heightened the vulnerability of businesses to cyber attackers leveraging high-speed broadband systems
- The ascent of mobile technologies and cloud computing, which has expanded the volume of sensitive business information liable to unauthorised access
- The growing technological sophistication of cyber attackers, whose ability to operate with speed and stealth exceeds the defensive capacity of businesses anchored to traditional IT security systems

Cyber crime is an asymmetric conflict that favours attackers over defenders. Cyberspace has no physical boundaries, and offers easy entry to individual hackers and small groups who mask their identities while launching cyber attacks. Corporations often fail to detect and respond to an attack in a sufficiently timely fashion to contain the damage as they typically require days, weeks, or even months to mount an effective defence (i.e., discovering the security breach and restoring lost or damaged assets).

In view of this asymmetry, IT security experts have come to regard cyber crime as the "new normal" of global business. Corporate leaders must accept the inevitability of cyber attacks, and build security systems and procedures that can not only pre-empt attacks (cyber defence) but enable the organisation to withstand attacks when they succeed (cyber resilience).

Costs

Cyber crime imposes a number of direct costs on global companies:

- Theft of financial assets
- Loss of intellectual property
- Violation of confidential information
- Costs of recovering/restoring violated data
- Damage to company's reputation

Cyber attacks also generate significant opportunity costs: diversion of corporate resources from R & D and other value-creating activities to cyber security infrastructure; loss of sales to customers affected by security breaches; diminished capital flows from now risk-averse investors.

A June 2014 study by Georgetown University's Center for Strategic and International Studies (CSIS) ("Net Losses: Estimating the Global Cost of Cyber crime") estimates the global annual cost of cyber crime as $375–575 billion. This represents 15-20 percent of the value of internet-related business worldwide. The actual economic costs may be higher in light of widespread under-reporting of cyber attacks that reflects the reluctance of many corporate managers to disclose cyber events damaging to the organisation's reputation.

The CSIS study reports interesting variations by country. Measured as share of GDP, cyber crime costs are highest in Germany (1.6 percent), Netherlands (1.5 percent), Norway (0.64 percent), and the United States (0.64 percent). Among the OECD

countries, Japan (0.02 percent), Australia (0.08 percent), and New Zealand (0.09 percent) report the lowest relative shares of cyber crime. Cyber crime is growing in emerging economies like Brazil (0.32 percent of GDP) where internet penetration is rising amid weak regulatory and legal structures.

Targets of Cyber Attacks

Unsurprisingly, financial institutions represent the principal target of cyber attacks. An analysis by the Pokemon Institute ("Cost of Cyber Crime Study: United States") reported that the U.S. financial services companies incurred average cyber-related losses of $23.2 million in 2013. In August 2014, several American banks (including JPMorganChase) suffered coordinated attacks by cyber groups that infiltrated computer networks and appropriated large amounts of client information. Banks and non-bank financial institutions are ripe targets for financial theft-related cyber attacks by virtue of their asset size, public visibility, and volume of electronic transactions.

However, industries outside financial services are increasingly prominent targets of cyber crime. In the Pokemon study, U.S. defence companies rank closely behind finance in average company losses ($23.2 million in 2013). American defence companies are of obvious interest to cyber groups seeking proprietary information on U.S. military technology and business intelligence on the U.S. defence industry.

The energy and utilities industry is also a prime target ($21.0 million average losses in 2013), illustrating the vulnerability of power stations and electric grids to operational disruptions by cyber attackers. Retail companies have become victims of cyber attacks, demonstrated most dramatically by the data breach at U.S.-based Target Corporation in late 2013 that affected 70 million customers, generated $200 million in credit card losses, and precipitated the removal of Target's Chief Executive and Chief Information Officers. Other leading retail companies such as eBay, Home Depot, and TJ Maxx have been cyber victims.

Cyber crime is meanwhile penetrating key manufacturing industries. The cyber vulnerability of manufacturing was demonstrated by the 2010 infiltration of Iran's nuclear centrifuge facility by Stuxnet, a "cyber worm" developed by American and Israeli software engineers that altered the motor drive frequencies of hundreds of gas centrifuges and set back the Iranian nuclear programme for years. Technological advances, particularly mobile smart phones and embedded devices ("internet of things" - the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure), have simultaneously expanded the productivity potential of manufacturing and rendered manufacturing companies more vulnerable to cyber attack.

Conclusion: Commercial Opportunities in Cyber Risk Management

While cyber crime poses significant challenges to global companies across a broad range of industries, it also creates major commercial opportunities for providers of cyber security products and services.

The CSIS estimates the total addressable market for cyber security as $58.2 billion. This market includes security equipment, consulting services, managed security services, policy and compliance support, web management, intrusion prevention systems, internet firewalls, and forensic analysis. In addition to cyber security systems, global companies exhibit increasing demand for specialised services in organisational design, corporate governance, and human resource management to enhance their readiness to cope with the mounting cyber threat.

About RSM

RSM is a worldwide network of independently owned and managed professional service firms, providing audit, tax, accounting and specialist consulting services. With global reach and local perspective, RSM member firms connect with their clients to deliver innovative solutions, helping them to see further, adapt faster and grow stronger.

RSM spans the globe, with more than 700 member and correspondent firm offices in 112 countries worldwide and more than 35,400 people on hand to serve clients.

RSM is a member of the Forum of Firms. The objective of the Forum of Firms is to promote consistent and high quality standards of financial and auditing practices worldwide.

www.rsmi.com

RSM is the lead sponsor of the European Business Awards

RSM is committed to promoting quality and excellence in business and championing the role of the entrepreneur in today's world economy. We are proud to be the lead sponsor and corporate champion of the European Business Awards. Despite the difficult economic environment, Europe is home to some of the world's most exciting and innovative businesses and it is important that we recognise and learn from that success to inspire others.

European Business Awards™ | Sponsored by RSM Audit · Tax · Advisory

David Bartlett

Executive in Residence
Director of Global and Strategic Projects
Kogod School of Business
American University
Washington, D.C.