

Think Ahead

ACCA

Cyberwarriors with calculators

The role of
accounting and
finance professionals
in a company's
cybersecurity

By
Dr. Jonathan Hill



Letter from the president of Pace University

Technology is ever-present in our lives. So too, unfortunately, is the imminent threat of hackers and those who would do us harm. The costs associated with cyberattacks are staggering. People and companies lose between \$375 and \$575 billion annually to these acts. The loss of our collective peace of mind cannot be quantified.

In order for our nation to continue to prosper in a rapidly changing world we must diligently protect our public and private technological infrastructures and maintain the trust of the international community. The American government and private industry is investing significant resources in this area, and Pace University is proud to contribute to the effort by collaborating with public and private sector representatives on research and innovative strategies that will detect, prevent and respond to cyberattacks.

Pace's location in the heart of the nation's financial district makes us particularly sensitive to potential cyberthreats that could cripple our nation's economic recovery and hurt millions of Americans. Our research with the Association of Chartered Certified Accountants (ACCA) helps us stay out in front of emerging cybersecurity issues while our annual summit brings together some of the brightest minds and most influential thought leaders on the topic.

The field of cybersecurity is important to both our faculty and students. In fact, the number of incoming undergraduates and graduates to the New York City campus of our Seidenberg School of Computer Science and Information Systems has grown over the last three years – helped by the almost \$3 million Pace has received for scholarships and research that support cybersecurity study and research. Sponsors are asking for new programs and course in areas such as Hardware Cybersecurity and Healthcare Security.

Dr. Jonathan Hill's research, in partnership with ACCA, provides both a national and international perspective on how company policies, individual practices and internal communications play a significant role in preventing and responding to cyberthreats. We are very proud of his efforts and are confident that his work will contribute to a safer, more secure and prosperous America.

A handwritten signature in black ink that reads "Stephen J. Friedman".

Stephen J. Friedman
President, Pace University

www.pace.edu

Letter from the head of ACCA USA



The growth of cybercrimes across our nation and world has risen to astronomic and unprecedented levels in recent years. As technology advances, so has the threat of silent attacks that strike at the core of our technological infrastructure.

This year, it appears as if no one is safe from the virtual scourge of cyberterrorists, as major corporations and our governments have been inflicted. In one of the most recent strikes, foreign hackers gained access to the data of at least four million U.S. government employees.

Three years ago, the Association of Chartered Certified Accountants (ACCA) sought to highlight the urgent need for more muscular cybersecurity mechanisms by partnering with the prestigious Pace University and its Seidenberg School of Computer Science and Information Systems.

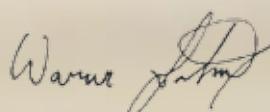
In fact, our decision to partner with a university based in New York City's Financial District was apropos: An 2012 ACCA survey found that worldwide, concern about cybercrime is disproportionately concentrated in the financial sector, and in particular, among large financial corporations.

Our partnership with Pace has since yielded three insightful cybersecurity summits, as well as a comprehensive report examining the global growth of "skimmer scams" that lift personal data from ATMs, gas pumps and cash registers.

Recognizing the fast-moving technological race that often sprints criminals ahead of businesses striving to protect their data, ACCA USA endeavored to better understand the scale of awareness and efforts among our members' companies. We undertook the following survey earlier this year, and its findings should be a wake-up call.

An initial step to implementing stronger controls is first understanding the seriousness of such cyberthreats, existing weaknesses in our infrastructures, and remedies that represent more than stopgap measures.

We applaud Pace University, President Stephen J. Friedman, and Dr. Jonathan Hill of the Seidenberg School of Computer Science and Information Systems, on their efforts to shed light – albeit a troubling one – on this virtual landscape.



Warner Johnston
Head of ACCA USA

www.accaglobal.com

Introduction

Computers, servers and the Internet are indispensable tools for financial professionals – and they are under relentless attack. For accountants, measures must be taken to ensure that the sensitive personal and corporate financial information they handle is safe: accountants need to be at the forefront of cybersecurity. This is particularly true today, as clients and consumers are more aware than ever of the cyber vulnerability of all businesses. Mistakes do not go unpunished: government leaders and legal authorities are focused on holding individuals responsible for breaches in cybersecurity.

The ACCA's second annual cybersecurity best practices survey, undertaken by the Seidenberg School of Computer Science and Information Systems at Pace University, indicates that ACCA members are adopting a range of strategies to cope with the challenges of maintaining a secure environment.

A survey of ACCA members

A survey of ACCA members garnered responses from a wide array of practitioners, managers and senior executives whose titles ranged from managing directors, CFOs, and senior VPs on the corporate level, as well as a variety of practicing accountants including practice managers, senior accountants and associates from both large generalist and smaller specialized public accounting firms. The responses indicate that financial professionals throughout the world are adapting to the sobering realities of a professional life where the raw materials of their trade – financial information including the sensitive financial data of companies and individuals – is the most prominent and desirable target for hackers and cybercriminals.

The survey reveals that the profession is adapting rapidly to adjust to the constant high threat level from a sophisticated, globally dispersed group of cybercriminals. However, communication between line managers and senior managers about attacks and attempted attacks needs to improve. In addition, the application of fundamental risk management cybersecurity practices needs to be applied more consistently throughout some firms.

Introduction

ACCOUNTANT AS TARGET AND DEFENDER

As FBI Director James Comey has said, "There are two kinds of big companies in the United States. There are those who've been hacked... and those who don't know they've been hacked."

Accounting professionals remain at the center of the threat because it is they who work with the data, the personal identifiable information (PII) that is the target for cybercriminals. Accountants work hand in glove with both internal cybersecurity professionals and external consultants to devise data security protections in the face of evolving threats from hackers. The ACCA maintains a robust research program on cybercrime and an ongoing dialogue on cybersecurity in the accounting and finance professions. They also engage with related organizations like Information Systems Audit and Control Association (ISACA) to craft best practices guidelines like the Control Objectives for Information and Related Technologies (COBIT 5) that address

the unique risks that come from the combination of responsibilities for financial control, risk management and computing technologies, including online vulnerabilities and device management.

LEGISLATION AND THE GROWING INVOLVEMENT OF GOVERNMENT

In the U.S. at least, it is a given that new regulatory guidance will be handed down from the government in the coming months. State and Federal lawmakers and regulators have asserted themselves in the wake of ongoing revelations involving cybercriminals hacking into the IT systems of major consumer-facing companies, including banks, major merchants, telecom companies and retailers. Even government agencies have found themselves the targets of relentless attacks. Companies are simultaneously being confronted by external threats from cyber thieves while being questioned by consumers uncomfortable with having their

PII transferred from businesses to government agencies. The desire for privacy and the need for secure data (and personal security) are increasingly in conflict in a world where cyber vulnerabilities are being identified on a daily basis.

In response to public demands for protection from cybercriminals, as well as business calls for protection from liability for cyber theft, authorities at the State level have moved to devise a standard of reasonable effort to which companies and their management would be held accountable. Legal action may be taken against firms and individuals who do not follow best cybersecurity practices.

By contrast, the U.S. House of Representatives passed two bills in April of 2015, which were combined into one bill that will be passed to the Senate: H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015, and H.R. 1560, the Protecting Cyber Networks Act. This now single

56%

of respondents in North America
are more concerned with cybercrime
than they were a year ago

38%

of respondents in Western European
are more concerned with cybercrime
than they were a year ago

bill would provide protections for companies that suffer a breach of consumer data, so long as those firms share their information security practices and customer data with Federal investigators. Where relevant, customers' PII would be stripped prior to being shared. A similar bill has already passed the Senate Select Committee on Intelligence – the S.754 Cybersecurity Information Sharing Act.

Previously, Cybersecurity legislation has been difficult to get through the U.S. Congress because of concerns about privacy and the potential cost of meeting yet another government mandated set of practices. However the present crisis and sense of vulnerability has left everyone – businesses, government and consumers – demanding that action be taken.

THE SAVVY CONSUMER

The onslaught of system hacks, data theft and cybercrime is unprecedented and overwhelming for both consumers

and financial professionals. Researchers estimate that two in five Americans have had their personal identifiable information stolen or have suffered unauthorized use of their credit cards. The news cycle each week seems to contain a new revelation about a major enterprise being hacked and millions of individuals' financial data being stolen.

Widely reported incidents detail the threats: criminals seeking to steal money; nation-state sponsored hackers seeking to destabilize government, finance and infrastructure systems; and non-state actors seeking to cause any damage possible.

This has left almost every enterprise's customer base or constituency jittery. Consumers are keen to do business with companies and agencies that can offer them a stronger assurance that their data will be protected and that their day-to-day commercial existence will not be interrupted by cybercrime or system shutdowns. However, many customers

are unwilling to go beyond the minimum to protect their own PII, preferring to leave the heavy lifting, and the blame, to businesses and organizations.

As user behavior often contradicts cyber safety etiquette, there is an inherent unfairness in being held responsible for the behavior of customers can essentially be their own worst enemies when it comes to protecting their own computers and mobile devices. Careless password management, clicking on any online link and the vulnerabilities inherent in connecting to every public Wi-Fi access point are the root causes of many cybersecurity breaches. Nonetheless, once a company takes possession of a user's personal data, it becomes the trusted agent responsible for securing that information.

SURVEY HIGHLIGHTS AND KEY INDICATORS

Pace University's Seidenberg School of Computer Science and Information Systems in New York devised an online

17%

reported that attacks were routinely reported to senior executives

Less than
50%

said breaches were reported to law enforcement

survey that was answered by a cross section of ACCA members including senior executives, consultants and sole practitioners, including auditors, accountants, directors, partners and consultants. The survey asked questions about company policy and personal practice in regards to cybersecurity. Importantly, it also asked about how evidence of cyberattacks was communicated within the firm.

Reporting attacks

The survey indicates a very real difference between internal and external reporting. Internal reporting often only goes as high as the next manager up in the reporting chain. Only 17% stated that attacks were routinely reported to the senior executives. As for reporting externally to law enforcement, less than 50% of respondents indicated that reporting is likely to occur in the event of a successful attack. This may indicate an unwillingness to 'go public' with news of a data breach that could adversely affect a company's reputation or even stock price.

Use of outside consultants

Nearly 50% of respondents indicated that it was somewhat or very likely that consultants would be hired in the wake of a cyberattack on their firm.

Reporting area for the cybersecurity function

There is an interesting spread among which 'C-level' officer the company's senior cybersecurity official reports to. 42% report to the CIO, 25% to the CEO and 17% report to the CFO.

Internal IT risk management policy compliance

While nearly 70% of respondents indicated that they had a high or very high level of awareness of their company's cyber risk management policies and procedures and 57% claim that their IT systems are well protected against cyberthreats, nearly a third (32%) have no knowledge of company policy on data encryption in transit or in storage. The results were similar for account access and management

protocols including password policies and procedures for the upload/download of software and documents. Furthermore, 31% of respondents indicated that there is no procedure for the removal of unauthorized software from employee machines.

In addition, adherence to the risk management protocols contained in internal corporate cybersecurity training and education programs are practiced by only 41% of the responding professionals.

Divergence on the Cloud

While two thirds of respondents indicated that they used and had great confidence in the integrity of their cloud server providers' cybersecurity practices, the remaining third do not use cloud storage at all, perhaps indicating that they feel safer using servers under their own control.

Nearly

50%

indicated it was somewhat or very likely that consultants would be hired after a breach

Nearly

70%

said they had a high or very high level of awareness of their company's cyber risk management policies and procedures

Adherence to COBIT 5

Fully 30% of respondents indicated that their firms did not follow the COBIT 5 framework at all while less than 10% said that their firms followed it stringently.

IT effectiveness assessment and audit/continuous improvement in response to an attack

The majority of respondents indicated that risk mitigation practices like vulnerability scanning and updating with software patches takes place regularly (71%). The more sophisticated (and intrusive) practice of penetration testing is practiced by about 40% of respondents. Nearly half (45%) perform security audits on a regular basis.

ACCA contributions

84.5% of respondents agreed that information provided by ACCA is somewhat or very valuable to them and their practice.

International comparison

As a global organization, the ACCA membership surveyed showed some

interesting differences between North American practitioners and their colleagues in the Middle East and Western Europe. 56% of respondents in North America are more concerned with cybercrime than they were a year ago, whereas only 38% of Western European respondents were.

A question regarding COBIT 5 adherence shows that 48% of North American respondents, 60% of Middle Eastern and only 43% of Western European respondents follow the COBIT 5 recommendations.

Confidence that the information systems they work with are secure was held by 63% of Western European respondents but only 47% of their colleagues in North America.

Encouragingly, 89% of North American respondents and 91% of Western European respondents indicated that it is easy for users to bring vulnerabilities to the attention of managers who can fix them.

Functional/job area comparison

The survey results point to a difference in perceptions in auditors and accountants. Auditors are more concerned about cybercrime today than they were a year ago (58% for auditors compared to 48% for accountants). Only 27% of accountants felt that their firm adhered to COBIT 5 standards whereas 43% of auditors believed their firms followed the standards.

57%

said their IT systems

are well-protected against cyberthreats

32%

had no knowledge of company policy on data encryption in transit or in storage

In conclusion

MERGING THREATS AND FURTHER QUESTIONS

This survey has generated data that is reflective of a profession that is adapting to a serious external attack on its processes and systems. The responses and needs of the main stakeholder groups – the financial profession, the IT profession and concerned government regulatory and law enforcement bodies – are evolving in response to progressing, ever more sophisticated threats.

There were some contradictions between the realities of day-to-day practice and the theory of cybersecurity best practices. As indicated by the cybersecurity breaches we hear about in the news every week, it is crucial that companies – and, especially, individual employees, begin to follow these practices. Techniques may vary from country to country; the survey indicated slight, but not insignificant differences in perception between practitioners in different regions of

the world. These differences centered around the perceived severity of the cybercrime threat and the security of the IT systems the practitioners work with. There were also interesting differences in perception between the accountants and auditors who responded.

In this environment there are as many questions as answers: is legislation coming? What will it look like? Will there be an enforceable COBIT? A Sarbanes-Oxley for data integrity? Who certifies which companies are safe? What is the certification or accreditation that says 'your data is safe'? The threat is so severe and protean that such a certification would be an inviting target for all hackers, black hat and white hat alike, who will be highly motivated to test their skills and beat this certification. If this is the case, how can such a certification prove a company is secure?

The immediate reality, however, is that accountants are under more pressure and consumers are worried

to the point where online commerce, banking and purchasing could slow after experiencing exponential growth. Government is, likewise, under pressure to respond and all of the defense and intelligence agencies have been tasked with meeting the cyberthreat. Businesses, including accounting firms, will lose clients to companies who seem 'safer' from a cybersecurity perspective. The at times uneasy working relationship between government and private industry will be tested as both parties are forced to integrate their activities, technologies and systems, leading to a call for a closer integration between Wall Street, Silicon Valley and the Beltway.

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants. It offers business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management. ACCA supports its 178,000 members and 455,000 students in 180 countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of 92 offices and centers and more than 8,500 Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conduct relevant research to ensure accountancy continues to grow in reputation and influence.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. It believes that accountants bring value to economies in all stages of development and seek to develop capacity in the profession and encourage the adoption of global standards. ACCA's core values are aligned to the needs of employers in all sectors and it ensures that through its range of qualifications, it prepares accountants for business. ACCA seeks to open up the profession to people of all backgrounds and remove artificial barriers, innovating its qualifications and delivery to meet the diverse needs of trainee professionals and their employers.

More information is available at www.accaglobal.com

About Pace University

Since 1906, Pace University has educated thinking professionals by providing high quality education for the professions on a firm base of liberal learning amid the advantages of the New York metropolitan area. A private university, Pace has campuses in New York City and Westchester County, New York, enrolling nearly 13,000 students in bachelor's, master's, and doctoral programs in its Dyson College of Arts and Sciences, Lubin School of Business, College of Health Professions, School of Education, School of Law, and Seidenberg School of Computer Science and Information Systems.

ABOUT THE LUBIN SCHOOL OF BUSINESS AT PACE UNIVERSITY

Globally recognized and prestigiously accredited, the Lubin School of Business integrates New York City's business world into the experienced-based education of its students at Pace's suburban and downtown campuses, implemented by the region's largest co-op program, team-based learning, and customized career guidance. Its programs are designed to launch success-oriented graduates toward upwardly mobile careers.

ABOUT SEIDENBERG SCHOOL OF COMPUTER SCIENCE AND INFORMATION SYSTEMS

Founded in 1983, the Seidenberg School of Computer Science and Information Systems at Pace University aspires to innovative leadership in preparing men and women for meaningful work, lifelong learning and responsible participation in a new and dynamic information age. The school does this through a broad spectrum of educational programs on campuses in New York City and Westchester County, and at other locations with corporate partners from the local and global community. As a National Security Agency certified Center of Academic Excellence in Information Assurance, the Seidenberg School offers bachelor's, master's and doctoral programs in computing to quality students from New York, the nation and the world.

www.pace.edu

Contact us

ACCA USA

150 East 52nd Street, 19th Floor
New York NY 10022

T: (212) 310 0105
F: (646) 304 1120
E: acca.usa@accaglobal.com

Follow us on Twitter @ACCA_USA
www.usa.accaglobal.com