CYBER AND PHYSICAL SECURITY:
PERSPECTIVES FROM THE C-SUITE

SURVEY RESEARCH PROJECT

Conducted by the Center for Cyber and Homeland Security (CCHS) in partnership with the International Security Management Association (ISMA)

Project Leadership

CCHS and McCrary Institute Director, Frank J. Cilluffo
CCHS Deputy Director, Sharon L. Cardash
CCHS Research Associate, Margaret W. Smith

ISMA President, David Komendat
ISMA Research Committee Chairman, Mike Howard

May 2019

ISMA
INTERNATIONAL SECURITY MANAGEMENT ASSOCIATION
The Global Association of Leading Chief Security Officers

AUBURN UNIVERSITY
CENTER FOR CYBER AND HOMELAND SECURITY

About Us

The Center for Cyber and Homeland Security (CCHS) at Auburn University is a nonpartisan think tank that works to develop innovative strategies to address current and future threats to the United States. We convene leading experts and practitioners for executive-level events, publish policy-relevant analysis, and provide expert testimony to Congress on critical issues and challenges related to cyber security, critical infrastructure, counterterrorism, and homeland security. The Center is part of the McCrary Institute for Cyber and Critical Infrastructure Security, and drives the policy component of the Institute's work.

The International Security Management Association (ISMA) is The Global Association of Leading Chief Security Officers – Assessing, Shaping and Evolving Corporate Security Risk Management Worldwide.

Foreword

Companies today face a remarkably wide array of risks from a broad range of sources. Physical security has always been a challenge in the world of "bricks & mortar"; and the "insider threat" is not a new concept either. Layering cyber threats atop this foundation, however, makes for a substantially (if not exponentially) greater and more complex risk portfolio. The need to manage that portfolio wisely begs the question of whether the C-suite has a combined and integrated approach to cyber and physical security (as well as risk more generally), or whether a more bifurcated tack remains widely adopted. With this project, CCHS and ISMA sought to explore the extent to which a combined/converged approach prevails, as well as the reasons for the answers to that question, and the drivers of the findings related to it. Our further hope is that this project will provide the beginnings of a roadmap and baseline for helping businesses to move forward smartly, given the significant uptick in investment in cyber security, recently, on the part of companies.

One caution however: as with any project of this nature, the findings must be appreciated in context. Accordingly, while our study revealed that Chief Information Security Officers are presently receiving more attention and more funding than Chief Security Officers, this is a function of the current climate of risk – and does not in any way detract from the longstanding and deeply valued contributions of CSOs. To the contrary, this particular finding actually underscores the achievements of the CSO community over time, in terms of maturing physical security (as distinct from cyber-related) programs and processes. Now, though, effective risk mitigation and resilience requires an intensity of focus on the cyber side, in order to grow, develop, and execute similarly robust programs and processes.

A number of individuals and entities were critical to the completion of this project. In particular, CCHS would like to thank ISMA for its financial and intellectual support and, especially, the time and insights of ISMA Executive Director Liz Chamberlin, ISMA Research Committee Member Lynn Mattice, and ISMA Membership Services Administrator Lacey Miller. The kind cooperation of Mike Stango and World 50, Incorporated; and Richard Ward and Edison Electric Institute; in assisting us to survey their member-companies was invaluable. Towson University Assistant Professor Dr.

Joseph R. Clark generously shared thoughts on the survey prior to its release and provided very helpful feedback on the draft paper that followed. CCHS Deputy Director Sharon Cardash was instrumental to the effort, managing it adroitly from inception to completion, and serving as contributing author and editor. CCHS Research Associate Margaret W. Smith was, likewise, crucial to the project in her role as principal author of this paper. Finally, CCHS Presidential Administrative Fellow and George Washington University graduate student Helen Christy Powell, and CCHS Interns/GWU undergraduate students Melissa Melvin and Matthew Edwards, each provided enthusiastic assistance on the technical dimensions of this project.[1]

Frank J. Cilluffo
CCHS and McCrary Institute Director

Mike Howard
ISMA Research Committee Chairman

[1] At the time of launch of this survey research project, CCHS was part of the George Washington University. Since then, CCHS has transitioned to operating under the auspices of Auburn University.

Bottom Line Up Front

The following benchmarking study, conducted by ISMA in partnership with the Center for Cyber and Homeland Security demonstrates that, in today's business environment, the role and activities of the Chief Information Security Officer (CISO) garner much of the attention of corporate Chief Executive Officers (CEOs). This is not to say that Chief Security Officers (CSOs) and the programs for which they are responsible go unvalued by CEOs. To the contrary, history underscores the importance of CSOs and their work. Currently, however, CEOs and corporate Boards of Directors are recognizing that a greater amount of dynamic risk attaches to cyber security-related matters than to physical security issues, in the near-term. As a result, the CISO is receiving more attention and more funding.

CEO Trends

- Respondents overwhelmingly prioritize cyber over physical security.
- All CEOs envision an increasing cyber security budget over the next five years.
- The CEOs surveyed believe they maintain a unified incident response plan that is a blend of cyber and physical security.

CSO Trends

- 85 percent of respondents believe senior leadership prioritizes cyber over physical security.
- Insider threat detection is important: 65 percent reported future innovations and changes in this technology will be "very significant" to their ability to carry out their responsibilities as CSO in the foreseeable future.
- Communication is key: 80 percent of CSOs surveyed report that improved coordination and information sharing with the CISO would expand their current operations and capabilities.

CISO Trends

- 71 percent of respondents view the shift to cloud-based services as having a significant impact on their ability to do their job over the next five years.
- From the CISO perspective, senior leadership prioritizes cyber over physical security.
- 72 percent of CISOs report conducting activities (such as presentations or training) designed to increase senior leadership awareness, understanding, and willingness to fund cyber security initiatives for their company.

Placing These Findings in Context

CSOs have had decades of visibility within the C-suite and with Boards of Directors, during which they have educated corporate leaders, matured security processes, and (in general) earned the confidence of CEOs.

After the attacks of September 2001, for example, CSOs began briefing their CEOs and Boards of Directors regularly about the risks associated with the asymmetrical and ever-evolving threat of terrorism. Lessons learned were widely shared and resulted in CSOs and corporations placing significant emphasis upon enhanced personnel screening, improved physical security, comprehensive travel security measures, strengthening business continuity programs (to ensure resilience), improved crisis management training, and employee mass-notification procedures.

These various practices subsequently served as the foundation for the emergency preparedness and response efforts that followed 9/11, including both mass-casualty workplace-violence incidents and weather-related natural disasters.

By comparison, programs for risk mitigation and effective resilience on the CISO side are at an earlier stage of maturity. Yet the internal and external threats and challenges that CISOs face are presenting at a dizzying rate, including relentless attacks against corporations by nation-states and cyber-criminals alike.

Managing the risks that inhere in such a complex and ever-changing environment is extremely difficult. Developing the measures, methodologies, and programs needed to protect and secure information technology systems and networks, and the data resident therein, will require sustained focus and leadership. It is against this background that the relative salience of physical and cyber security indicated by the survey should be understood.

Overview

Introduction

The Center for Cyber and Homeland Security (CCHS) together with the International Security Management Association (ISMA) conducted a survey research project to examine how C-Suites view and manage physical and cyber security within their respective companies and across the global community.

The study sought to determine whether physical and cyber security are viewed and treated as combined and/or integrated within an organization; or whether they are approached as two distinct and bifurcated functions.

Objectives

The objective is to illustrate how C-suite executives (specifically: CEOs, CISOs, and CSOs) understand physical and cyber security within their organizations; and the extent to which security is viewed and undertaken either as a holistic function – or – to the contrary, if physical and cyber security are approached separately.

Methodology

The Survey

The survey link was shared via email with members of the International Security Management Association (ISMA)[2], World 50 Inc.[3], and Edison Electric Institute (EEI)[4].

- ISMA members (CSOs) were invited to share the survey with their CEOs to request their participation.
- World 50 members included CISOs from top-tier global companies; again, participants were asked to share the survey with their CEOs to gather their perspectives as well.
- EEI members included CSOs and CISOs.
- EEI members were selected as part of the respondent pool because the organization represents a truly critical (infrastructure) sector.

[2] ISMA membership base includes roughly 400 executives (CSOs and CEOs) from major corporations spanning five continents and collectively representing some 20 percent of the Fortune Global 500 including 25 companies in the FTSE 100, DAX, and CAC 40. Additionally, members represent more than 50 percent of the Fortune 100 and 25 percent of the Fortune 500. Membership requirements are twofold: 1) security practitioners need to be the senior security executive whose primary responsibility is the development of security policies and controls for an organization with annual revenue exceeding 1 billion US dollars or its local equivalent or 2) CEOs of a security services supplier are eligible for membership if the company supplies a full range of consultative security services and has annual revenue exceeding 100 million US dollars or its local equivalent. Additional information on ISMA members can be found here: https://isma.com/Membership

[3] World 50 is a private community for senior-most executives by function primarily from the large multinational companies of the Global 2000. Membership is invitation only. Additional information about World 50 can be found/requested here: https://www.w50.com/https://www.w50.com/

[4] EEI is the association that represents all U.S. investor-owned electric companies. EEI members provide electricity for about 220 million Americans and operate in all 50 states and the District of Columbia. Additionally, EEI has more than 60 international electric companies with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members. There are three categories of membership: 1) U.S. Investor-Owned Electric Companies, 2) International Members, and 3) Associates. Additional information about EEI and its members can be found here: http://www.eei.org/about/members/Pages/default.aspx

The cover note sent to recipients of the survey link read as follows:

> *The George Washington University Center for Cyber and Homeland Security [now part of Auburn University] together with the International Security Management Association is conducting a survey to examine how C-suites view and manage physical and cyber security within the enterprise. Your participation--and also the participation of your company's CEO--is critical to the value of this survey. Please forward the survey link to your CEO and endeavor to convince him or her to participate in this very short survey.*
>
> *The survey seeks to determine whether physical and cyber security are viewed and treated as a combined and integrated organization; or whether they are approached as two distinct and bifurcated functions. Regardless, the survey seeks to understand the drivers for the approach adopted.*
>
> *Key findings will be shared in a report. Both survey and report will maintain respondent anonymity and privacy. The ultimate goal of both survey and report is to help businesses enhance both physical and cyber security. The survey will remain open for five business days.*
>
> *The input of both you and your CEO is critical to the success of the project; and we would be grateful if you might share the survey questions with your CEO so that they might respond, in addition to yourself. Thank you so very much for your time, help, and consideration.*

The data collected is intended to provide a description of how C-Suite professionals perceive security and if they approach cyber and physical security as a unified effort.

Data Collection

This study used Survey Monkey for data collection. The questions were multiple choice, closed response, with the option to select "Other" which prompted the ability to enter an open response if none of the choice categories aligned with a participant's organization. The survey was kept open for one month after the initial email (details on timing are listed below) and the participant was required to complete the survey in a single sitting.

All participants answered an initial set of three questions to identify the size of their organization by number of employees and the industry sector in which it operates.

Finally, the participant was asked to select their title/job role before being directed to questions specific to CEOs, CISOs, and CSOs. CEOs answered an additional 10 questions about their role, company, and security operations for a total of 13 responses; CISOs answered an additional 10 questions for a total of 13 responses; and CSOs answered an additional 10 questions for a total of 13 responses.

Timing

The "survey launch date" is the date of outreach to members of the respective organizations with an email containing the survey link. The "survey close date" is the date of termination of the survey. Respondents had roughly one month to complete the survey. Given the lengthy survey window, we conducted a search for any intervening events (potential stochastic shocks) occurring between January 18 and February 12, 2018, that could have created a situation in which respondents that answer before an event generally have a different opinion than those who answer after an event. First, a search was conducted for breaches of cyber or physical security in the United States, specific to the sectors surveyed in this report. During this search, no physical security breaches were found. A second search checked for international incidents without limiting the search to the sectors surveyed in this report. Based on the search results, we do not believe the highlighted events had a significant impact on respondents' opinions; however, please see the Appendix for the breaches identified during the search.

Table 1: Launch Dates and Timing

Survey Timing		
Entity	**Survey Launch Date**	**Survey Close Date**
ISMA	Thursday, 18 January 2018	Monday, 12 February 2018
World 50	Monday, 22 January 2018	Monday, 12 February 2018
EEI	Tuesday, 23 January 2018	Monday, 12 February 2018

Respondent Pool

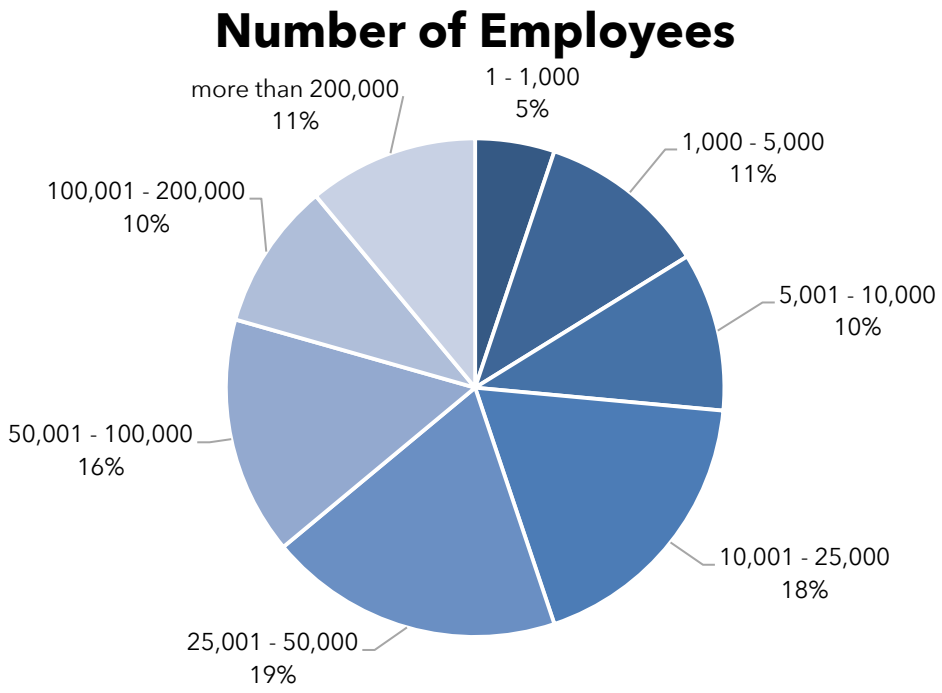
136 responses were received from individuals affiliated with the three, targeted entities. Responses were provided anonymously and it was not possible to trace individual replies back to their originating organization. Respondents' professional experience spans multiple sectors. The top five sectors represented in the respondent pool were:

Table 2: Top 5 Industries Represented in Respondent Pool (N = 136)

Industry	% of Respondent Pool
Banking/Financial	11.19%
Manufacturing/ Fabricated Goods	11.19%
Utilities	10.45%
Retail	8.21%
Communications/Telecomms.	7.46%

Additionally, respondents primarily came from organizations with more than 1000 employees, with the greatest number falling between 10,0001 and 50,000 (38 percent combined).

Figure 1: Company Size by Number of Employees



Finally, the respondent pool was comprised of 8 percent CEOs, 13 percent CISOs, and 80 percent CSOs.

Notes on Interpretation

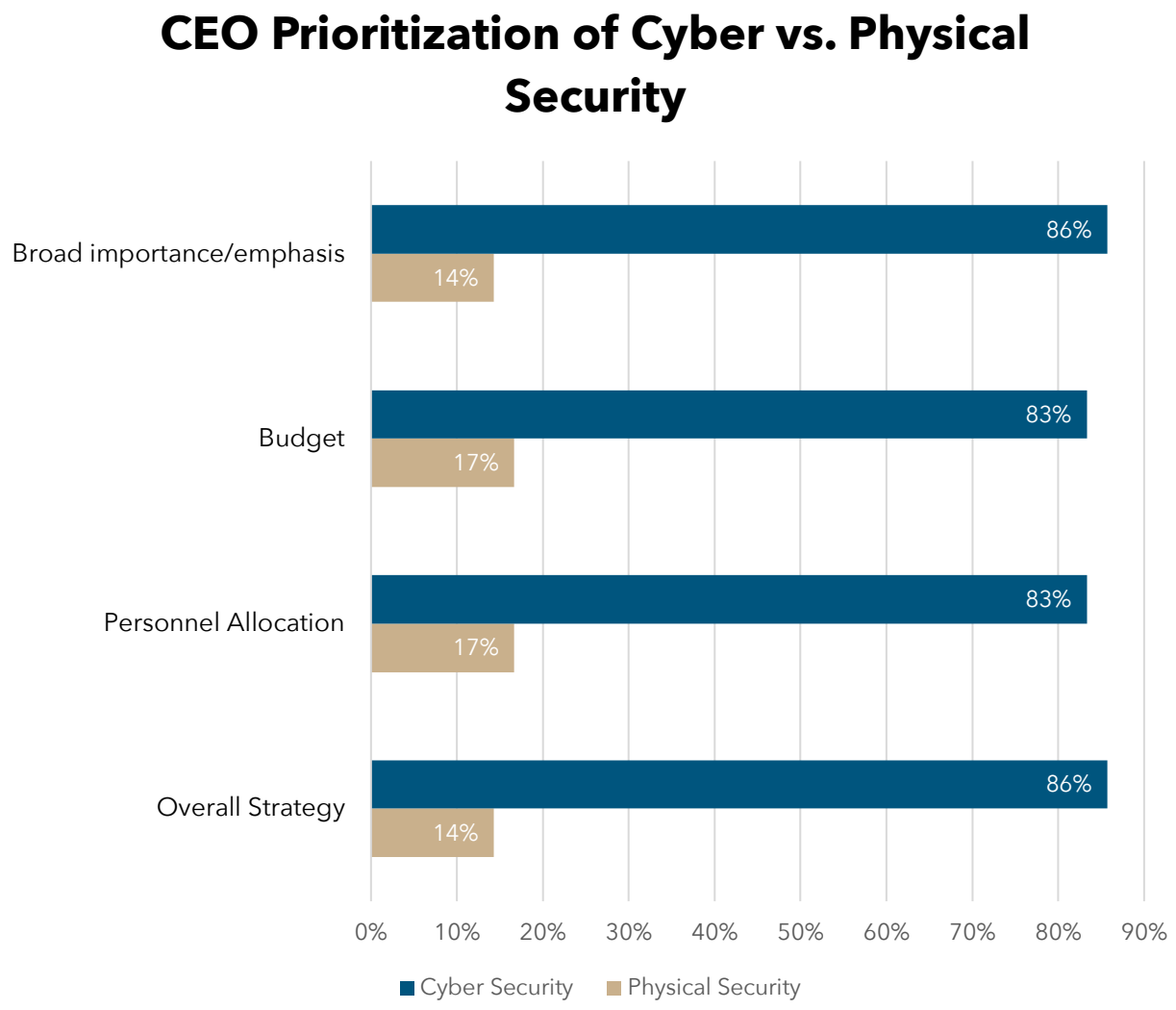
Before presenting the survey findings, it is important to note that the sample size, while sizeable (N = 136), is divided between work role, limiting responses for questions aimed at CEOs, for example, to nine. The responses (not every respondent answered every question) and results below represent the perspectives of a relatively small population of CEOs, CISOs, and CSOs, raising questions about generalizability from a statistical standpoint. However, since our target population is quite narrow in scope (senior-level corporate executives), the study's small sample size is likely to be representative of the greater population of C-Suites as a whole. Additionally, as C-Suite professionals and members of ISMA, World 50, and EEI, the respondents are positioned to provide key information about how cyber and physical security priorities are considered. These individuals, as a group, understand the choices associated with security prioritization, budgetary constraints, external pressure, and other factors influencing how an organization implements both cyber and physical security measures. For that reason, ISMA, World 50, and EEI members were judged to be the best target population for this online survey. Based on this, and the fact that the primary goal of the survey was the collection of descriptive statistics about C-suite security trends, the sample size and varied response size of this dataset is not considered a methodological flaw. Any future surveys should, though, expand the sample to gather a more evenly distributed pool of C-suite professionals to allow for more robust discussion about trends and to potentially enable greater confidence in the conclusions drawn from the data.

Results

CEO Data

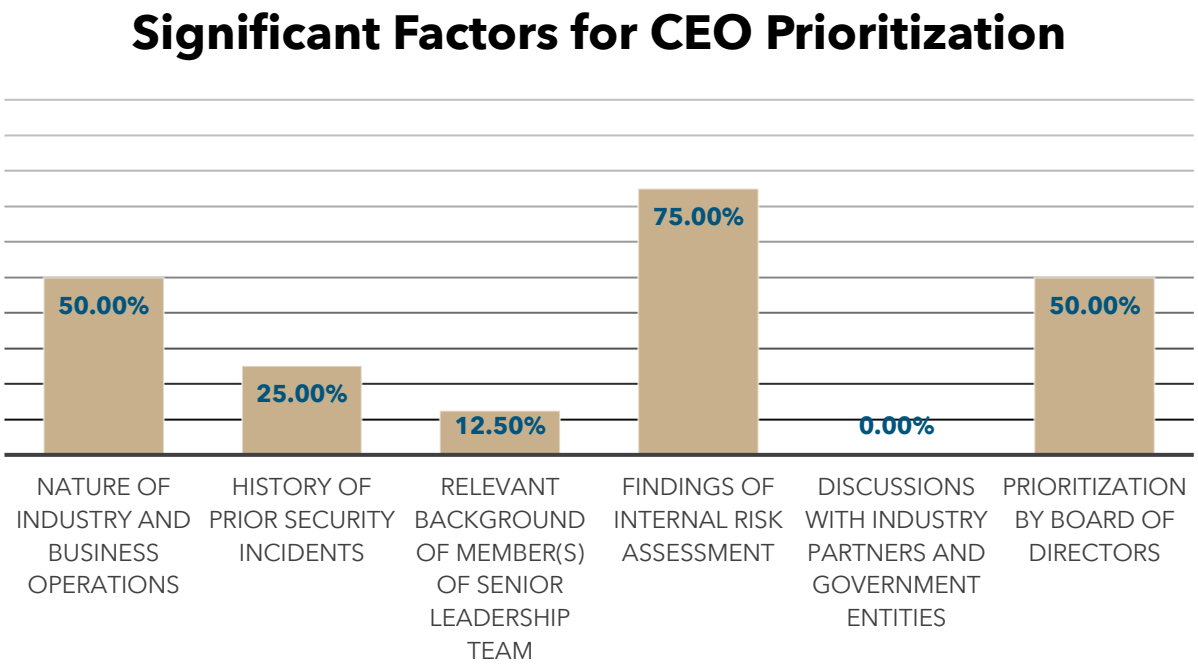
CEOs overwhelmingly prioritize cyber over physical security with regards to importance, budget, personnel allocation, and overall strategy.

Figure 2: CEO Prioritization



As detailed in Figure 3 below, the respondents selected "findings of internal risk assessment" as the most important driver of their strategic emphasis on cyber security while none found "discussions with industry partners and government entities" to be significant.

Figure 3: List of Significant Factors for CEO Prioritization

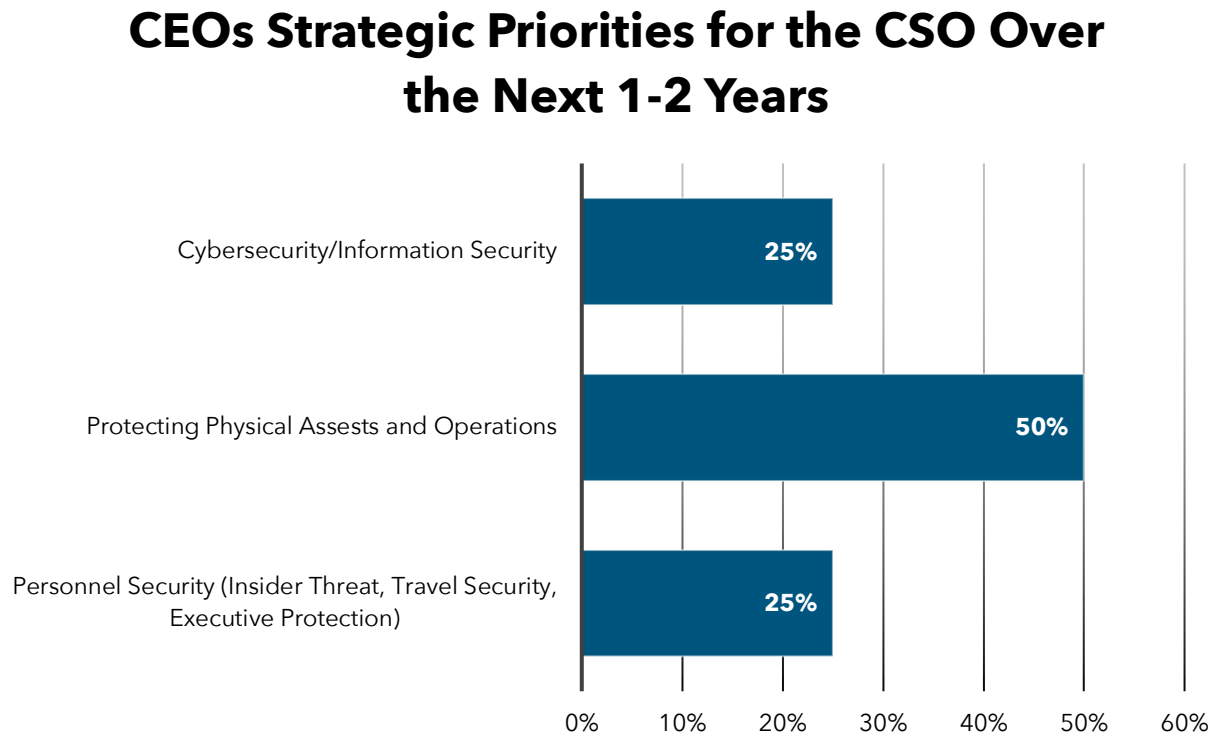


Complementing the strategic emphasis on cyber security, all CEO respondents envision a steadily increasing budget for cyber security initiatives. Only 29 percent predict a similarly increasing budget for physical security initiatives. Despite a weighted focus on cyber security, the CEOs surveyed believe they maintain coordinated or unified incident response plans, indicating the companies intend to take a holistic view of security rather than drawing distinct lines between cyber and physical security efforts. Therefore, increasing cyber security budgets are not seen as taking away from a company's physical security efforts; the unified incident response plans attempt to balance company needs based on internal risk assessments and weight funding accordingly.

Despite 71 percent of CEO respondents indicating that they do not envision a steadily increasing physical security budget for their company over the next 5 years, 50 percent of the same respondents selected "protecting physical assets and operations" as their most important priority for the CSO over the next 1-2 years. 25

percent of respondents viewed "personnel security" and "cyber security/information security" as the priority. However, it is not clear how the respondents understood the answer choices. "Operations" can also be understood as an online function (i.e. cyber operations) within a financial firm, for example; and "physical security" includes "insider threat" as one of its subcategories, which can also be understood as a cyber threat. Therefore, despite prioritizing the protection of physical assets and operations over 50 percent of the time, CEO respondents could be thinking of cyber threats within those answer categories.

Figure 4: CEO Strategic Priorities for the CSO



Of the CEOs surveyed, none receive direct reporting from their CSO or CISO. All CEO respondents indicated that their company maintains a CSO or a CISO and that they meet more frequently with the CISO because their responsibility for cyber or physical security is a relatively important role within the company. Corporate structure, however, appears to differ dramatically as the CEO respondents indicated different reporting pathways for whom the CSO or CISO reports to within the company.

Figure 5: Reporting Lines for CSOs

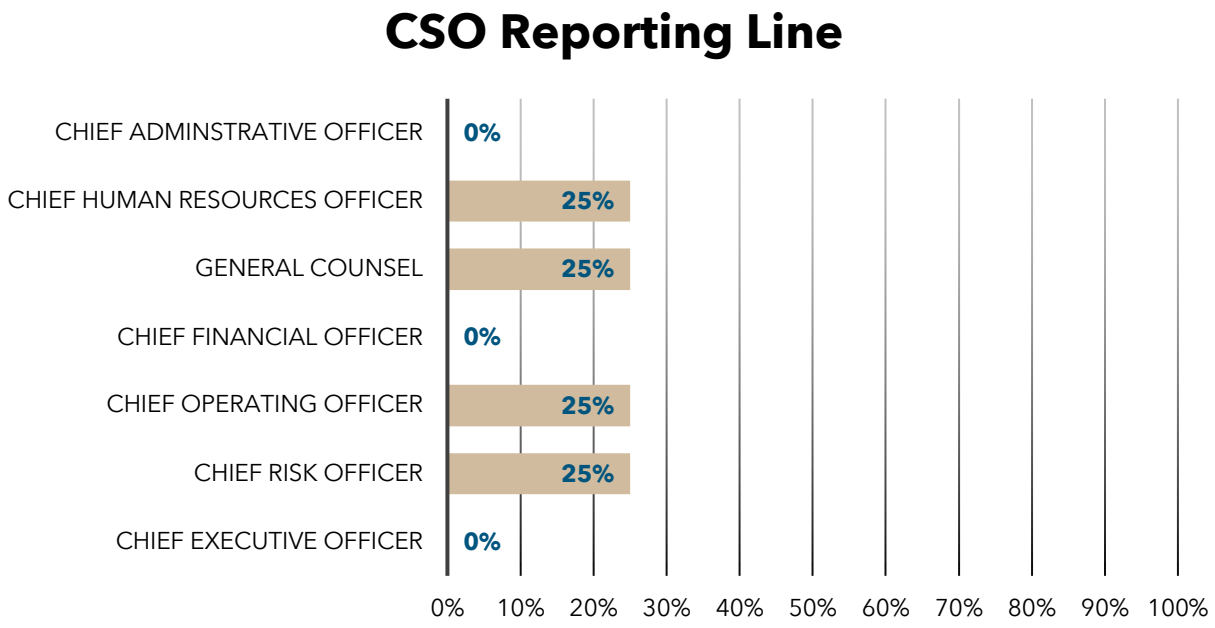
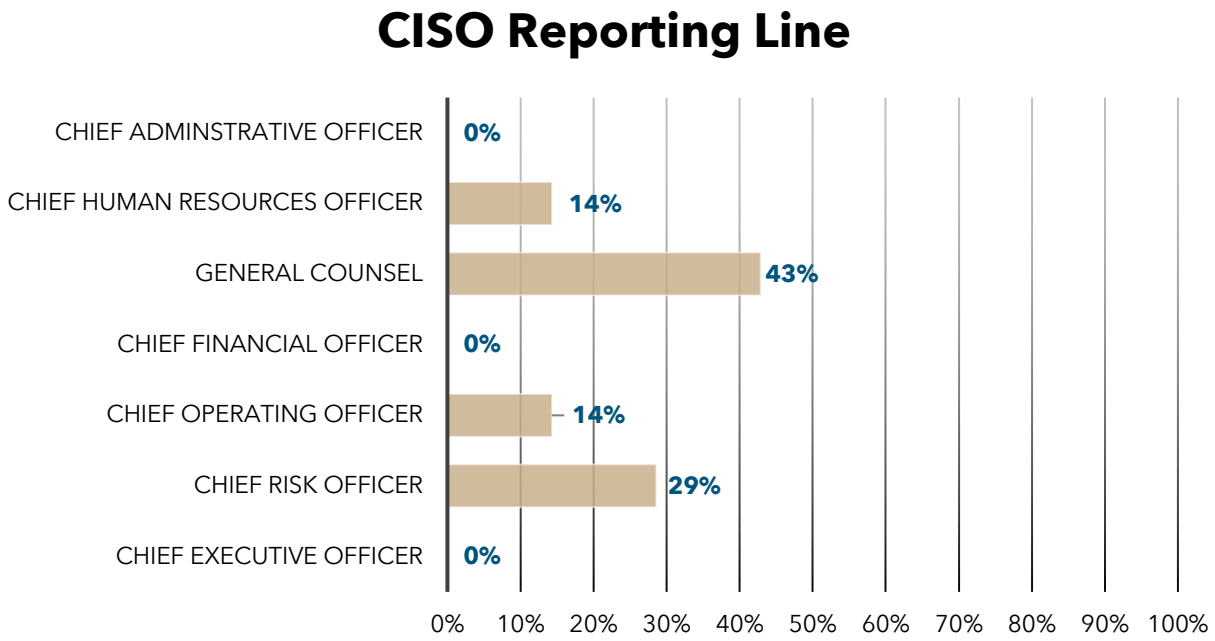


Figure 6: Reporting Lines for CISOs



Overall, the CEO respondents prioritize cyber security based on a current understanding of company risk. Yet, despite predicting that cyber security budgets will increase in the next few years and despite emphasizing cyber security initiatives, the CEO respondents report a combined approach to security through unified incident response plans intended to integrate physical and cyber threat response.

CISO Data

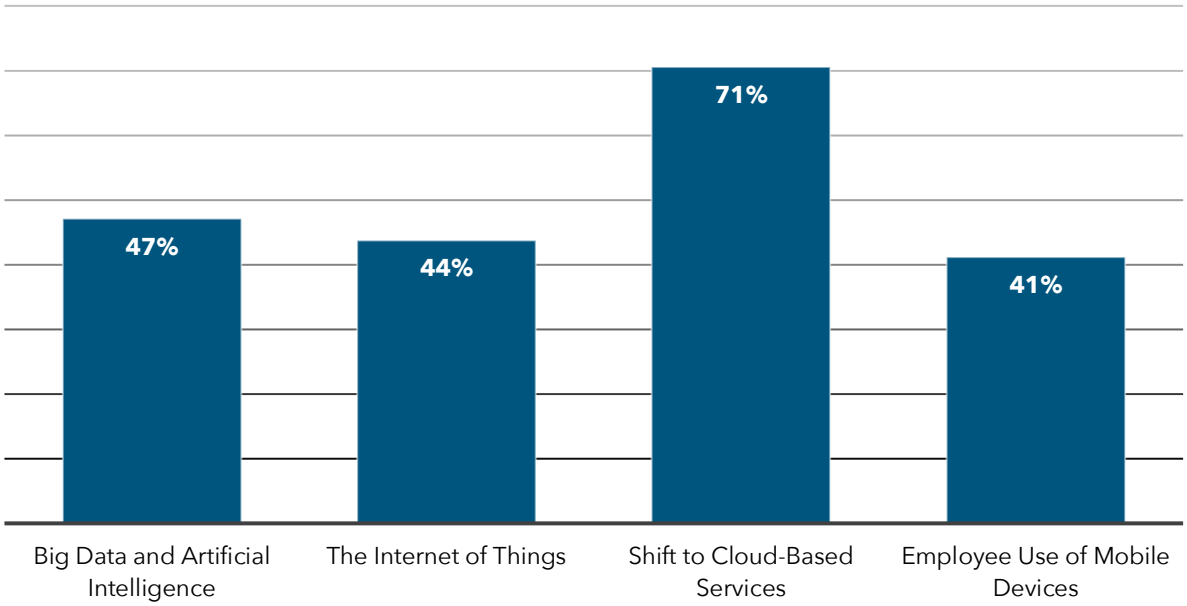
From the CISO perspective, senior leadership prioritizes cyber security over physical security. Additionally, 44 percent of respondents highlight recent cyber security incidents as a reason for senior leadership's prioritization. CISOs are also actively involved in enhancing their senior leadership's understanding of cyber threats which could account for their increasing focus on cyber security. 72 percent of CISO respondents did two or more of the following:

- Made presentations on cyber threats at senior leadership meetings and/or board of directors' meetings.
- Brought in outside cyber security experts to speak to senior leadership or board of directors.
- Held tabletop exercises with senior leadership of company on cyber threats.
- Implemented penetration tests of company and provided results to senior leadership.
- Developed new employee training on cyber threats and risks.

These activities appear to increase senior leadership awareness, understanding, and willingness to fund initiatives to improve cyber security. 77 percent of CISO respondents envision growing cyber security budgets over the next few years while only 33 percent predict an increase in the physical security budget. However, 70 percent reported having a unified incident response plan that incorporates a coordinated effort between physical and cyber security. This unification again implies a holistic view of security despite the existing budget and prioritization differences.

Within their respective companies, 72 percent of CISOs surveyed report directly to the CIO and 82 percent selected that they have a "strong working relationship" with that office. Additionally, the CISO respondents selected "moderate to strong working relationships" as the category that best describes their relationship with their company's CSO. However, the majority also selected that this relationship could be "enhanced or improved through greater information sharing and improving the coordination and planning between the CSO and CISO offices." In addition to improved communication between the CSO and CISO offices, 71 percent of respondents view the shift to cloud-based services as having a significant impact on their ability to carry out the responsibilities of CISO in the next five years.

Figure 7: Technology/Innovations Predicted to Have a "Very Significant Impact" on CISO Effectiveness in the Next Five Years



Overall, from the CISO's perspective, cyber security is leadership's priority. CISO efforts to increase awareness of cyber security threats and best practices through exercises that directly engage senior leadership indicate that as the perceived threat increases, CISOs are making efforts to ensure they have the support required to maintain the resources necessary to counter new and evolving threats. A desire for greater coordination and cooperation with CSO offices could indicate a need for a more unified approach to security, or a sense that greater unification of efforts could lead to an improved security posture.

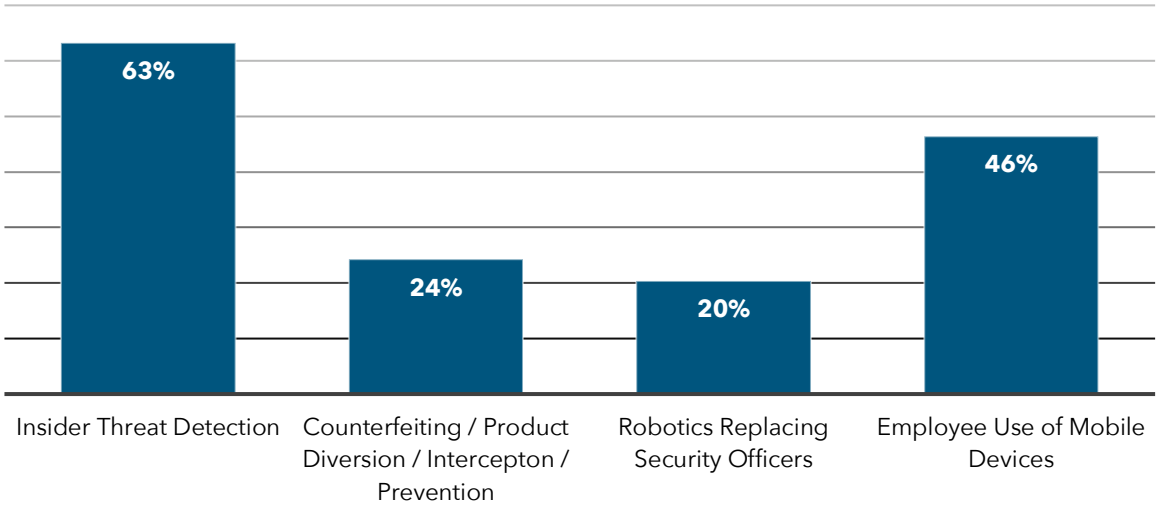
CSO Data

From the CSO perspective, 85 percent of respondents believe senior leadership prioritizes cyber security over physical security. In addition to inherent business reasons for prioritizing cyber security, 70 percent of the respondents highlighted recent cyber security incidents as a reason for senior leadership's prioritization. CSOs perceive that senior leadership's focus on cyber security over physical security is due to their companies experiencing more cyber security incidents than physical security incidents in the recent past. CSOs also actively seek out ways to enhance their senior leadership's understanding of cyber threats with over 85 percent having made

presentations on threats to the business at senior leadership meetings and/or board of directors meetings.

The majority of CSO respondents, nearly 60 percent, envision growing security budgets over the next five years and roughly 70 percent reported having a unified incident response plan that is a coordinated effort between both physical and cyber security. With growing budgets, CSOs appear hopeful that innovations will occur in the area of insider threat detection; nearly 65 percent of respondents indicated changes in this type of technology will be "very significant" to the ability to carry out their responsibilities as CSO in the next five years. Additionally, employee use of mobile devices was cited as being "very significant" to a CSO's ability to carry out their responsibilities, by over 45 percent of respondents. Because it is unclear from the survey data whether CSOs view this technology as enhancing or hindering their ability to carry out their responsibilities, future research should investigate how mobile technology both enhances and hinders cyber and physical security efforts.

Figure 8: Technology/Innovations Predicted to Have a "Very Significant Impact" on CSO Effectiveness in the Next Five Years



Within the company, most CSOs surveyed report directly to the General Counsel and maintain a strong working relationship with that office. An interesting line of future inquiry would be to better understand this working relationship and how corporate structure can facilitate a dynamic and effective security posture. Additionally, 80 percent of the CSO respondents report having "moderate to strong working relationships" with their company's CISO. However, CSOs also find that improved

coordination and information sharing with the CISO would expand their current operations and capabilities.

Key Takeaways

Over the next five years, C-suite professionals envision increasing security budgets to address the rise in threats and incidents. These increases are weighted towards cyber security; however, survey results do not indicate a diminishing role for physical security. Instead, respondents tended to report a unified security plan. One possible explanation for this trend towards holistic security is the hybrid threat: for example, a perceived threat among the C-suite professionals surveyed for this report is the insider threat — something that has implications for operations in the real and virtual worlds, and therefore requires a unified response and security plan. The integrated approach, as indicated in the survey results, will require greater coordination and information sharing between CSO and CISO offices to ensure their respective agendas complement rather than hinder one another's operations.

An interesting opportunity for future research has been identified through this study. Investigating if and how external security incidents or breaches influence a C-suite professional's approach to security could help identify new opportunities for collaboration and a greater sharing of best practices among executives. Understanding how executives learn from global security incidents that impact other companies, how those incidents impact their own operations, and if/how they prompt or influence C-suite-level change can influence how and what information is shared.

One-on-One Interviews

Introduction

In complement and supplement to the survey, a select number of one-on-one interviews were conducted with C-suite executives in order to identify and highlight certain notable best practices in regard to the treatment and pursuit of cyber and physical security. In some but not all instances, the individual/company interviewed agreed to be named herein; only details for which consent-to-publish was received appear below.

Northrop Grumman Corporation, Vice President & Chief Information Security Officer, Dr. Michael Papay:

At Northrop Grumman, corporate security policy is jointly owned by the CSO and CISO, who are co-responsible for the elaboration and execution of the majority of the company's (security) policies. Moreover, the CSO, CISO, and CIO are peers of one another. All three fall under the Sector President for Enterprise Services. In practice, these three Chief Officers meet weekly via teleconference, and quarterly face-to-face, in order to conduct strategic planning.

The CSO and CISO lead the company's larger Corporate Security Council - established in 1987 and including Legal, HR, and other components – which is where further deconfliction and prioritization of efforts takes place. The Council manages key security risks and concerns. The Board of Directors receives briefs from the CSO and CISO on a regular basis. The Corporate Security Council facilitates the alignment of cyber/information and industrial security, as does the approach of both the CSO and CISO who view everything through a single lens - that is, risk - and then pull the pieces into a single dashboard that offers a cohesive assessment.

Northrop Grumman has worked to adopt a proactive posture that seeks to bake in security at the front end and align it to business processes (rather than have security of any type be relegated to "a footnote" at the back end). At the same time, the

government insider threat requirement has driven many of the company's security measures; and insider threat detection has brought the physical/industrial and cyber/information security teams even closer together.

Large Multinational Company, Security and IT

An identified best practice for developing and executing an effective cyber security strategy in a large multinational company with global presence is to establish a collaborative, bifurcated model that delivers an information protection capability through the partnership of two functions: Security and IT.

Security is responsible for maintaining oversight through a holistic approach that focuses on the protection of the company's assets: information, products, financials, people, and infrastructure. With regard to information protection, Security is responsible for establishing the company's policy and managing exceptions; IT security must then ensure compliance. Security also has the more traditional aspects of asset protection: intelligence gathering (re: threat actors and trends, and geopolitical risks); investigations; and external liaison.

The two functions (Security and IT), together with other business and headquarters representatives, form a steering committee that discusses IT strategy (e.g., moving to the cloud) and identifies risks to the business. These risks are provided to the company's leadership in order to better inform business decisions and ensure that they have a tolerable risk/benefit ratio.

APPENDIX

Intervening Incidents – U.S. Search Results

Sector	Incident	Date
Banking/Financial Services	○ Frost Bank in Corpus Christi (a subsidiary of Cullen/Frost Bankers Incorporated): 470 commercial customers of the bank had their account's security breached. Unauthorized users viewed and copied electronic images of checks. FBI and U.S. Secret Service are investigating the breach.	2/18
Defense Industrial Base/Government Contractors	○ The Marine Forces Reserve: 21,426 people affected by a data breach. An email with personal confidential information sent unencrypted; information included social security numbers, bank routing numbers and electronic funds transfer information, mailing and residential addresses, and emergency contact information.	2/12/18
Education/K12	○ The Florida Virtual School (FLVS) Program: an estimated 368,000 students and 2,000 teachers affected during a two-year data breach; information included student and parent names, dates of birth, email addresses, and school account numbers. ○ Nampa (Idaho) School District: announced a breach of its system by an individual with unauthorized access; the information of almost 4,000 employees was potentially affected (investigation ongoing).	5/2/16 – 2/12/18
Education/University	○ University of Alaska: announced a data breach affecting 50 accounts of employees and students.	2/27/18
Miscellaneous	○ Applebee's: reported that between December 6, 2017, and February 13, 2018 - when the breach was discovered, there was malware present on the systems of more than 160 restaurants in multiple states; the malware was designed to collect information of credit cards run through the payment system; names, credit and debit card numbers, expiration dates, and verification codes were affected.	2/13/18

Intervening Incidents – International Search Results

Sector	Incident	Date
Banking/Financial Services	Russian servers linked to DDOS attack on Dutch financial network, including ABN Amro, ING, and Rabobank; the perpetrators used a botnet to conduct the attack.	End of January 2018
Banking/Financial Services	Hackers broke into Japan's Coincheck Inc. cryptocurrency exchange and stole nearly $500 million in digital tokens; the attack was not attributed.	End of January 2018
Government	German news reported that Russian hackers breached the online networks of Germany's foreign and interior ministries. The breach was undetected for a year; according to officials, the breach became known in December 2017.	2/18
Healthcare (Hospitals & Medical Centers)	ATI Physical Therapy experienced an email hack that resulted in the exposure of data of 35,136 patients; compromised data included social security numbers, health insurance ID numbers, and medical records.	1/9/18 – 1/12/18
Nonprofit	Two Ontario-based children's aid societies made public that they were the victims of ransomware attacks; Children's Aid Society of Oxford County stated its local servers were hit on January 18; and Family and Children's Services of Lanark, Leeds & Grenville stated their computers had been hit with a similar ransomware attack in November 2017.	1/18/18
Passenger Transportation	Metrolinx, a transit agency based in Ontario, Canada, stated that the company had been attacked by North Korea, via a virus (that was routed through Russia); but a spokesperson for the company stated that neither safety systems nor privacy had been compromised or breached.	1/23/18
Retail	The card numbers of customers at Saks and Lord & Taylor stores were stolen through malware installed in the stores' checkout systems; the majority of stores targeted were located in New York and New Jersey	5/17 – 3/18
Spectator Sports (Leagues/Events)	Cyberattack during the Opening Ceremonies for the Pyeongchang Olympics; disrupted the Games' internet service, broadcast systems, and website.	2/19/18
Utilities (Electric, Gas, Nuclear, Water)	Infection of a water utility in Europe: the attack is the first discovery of an unauthorized cryptocurrency miner impacting industrial control systems or SCADA servers.	2/18
Vehicle Manufacturers	Porsche Japan stated that more than 28,000 email addresses had been leaked as the result of a hack; in addition, customers' names, addresses, phone numbers, and income information may have been compromised.	2/26/18