Deloitte.

The cybersecurity talent shortage

An emerging challenge for consumer products companies

Cyber Risk

Executive summary

Cybersecurity threats are all too common in today's digitally connected world. Recent major cyber breach incidents that highlight the seriousness of the issue include shadow brokers threatening to expose NSA data; ransomware called "WannaCry" spread around the world; and WikiLeaks CIA Vault 7, which has led to debate about the risks inherent in government development of digital spy tools.[1]

In the world of consumer products (CP), as discussed in recent Deloitte publications, "Cyber risk in consumer business" and "Why CMOs should care about cyber risk," consumer businesses are often inadvertently opening the door to cyber threats. How? By investing in newer technologies that have not been fully considered from a cyber risk perspective due to the need to quickly implement them in today's hypercompetitive, fast-paced marketplace. These newer technologies typically include developments in customer analytics, cloud integration, connected devices, and digital payment technology.[2]

It commonly falls upon the shoulders of cybersecurity professionals to be proactive in helping to prevent and predict cybersecurity breaches. It is often of critical importance to have the right employees, focused on the right tasks, to mitigate cyber risk.[3] Similar to other industries, CP companies can have a difficult time attracting, hiring, and maintaining top cybersecurity talent. There are many common and cross-industry factors contributing to this predicament, such as:

- The demand for skilled cyber talent far outweighs the available talent pool
- The challenges of sourcing talent with the right skill set
- The tendency to recruit talent with traditional education backgrounds and experiences, or who have security certifications
- Women being underrepresented in the cyber workforce

CP companies face an additional challenge of attracting talent to their organizations due to the perception among younger workers that CP careers aren't as stimulating as they once were.

The ability of CP companies to promote a culture of security through proactive, organization-wide engagement and implementation is likely dependent on their ability to attract and retain cyber talent to implement cybersecurity programs. CP companies can take proactive steps to help ensure that highly skilled cyber professionals are at the helm of their cybersecurity efforts. To attract top cybersecurity talent, CP companies could benefit from:

- Implementing measurable cybersecurity learning and awareness programs within their organizations
- Appealing to Millennial and future Gen Z workers (who fuel the pipeline of cybersecurity talent) through a commitment to training and development, ensuring challenging work opportunities, offering targeted employee benefits such as flexible working hours and casual work environments, and demonstrating a commitment to social impact programs aligned with the interests of younger workers
- Exploring the sourcing of talent from nontraditional backgrounds that have relevant work experience
- Hiring more women and minorities
- Stimulating interest in cybersecurity careers by building early awareness among younger students (in high school and college)

Applying these principles to cyber talent in CP companies, as well as the lessons learned in Deloitte's "Cyber risk in consumer business report" (see sidebar), can help CP companies be **secure, vigilant, and resilient.**

Research methodology

Insights reported in this paper are drawn from Deloitte's "Cyber risk in consumer business" study. Deloitte launched this study to assess current challenges faced by companies in the consumer products, retail, restaurant, and agribusiness sectors. Using a combination of an online survey and in-depth interviews, opinions were gathered from more than 400 CIOs, CISOs, CTOs, and other executives in these sectors. Insights reported in this paper are drawn from a subset of 150 interviews with executives from the consumer products sector.

The continued threat of cybercrime

Cyber threats are not likely to disappear: It's estimated that the cost associated with cybercrime (at $3 trillion in 2015) will likely increase to $6 trillion by 2021.[4] In an attempt to address the magnitude of cybercrime, federal and commercial marketplaces plan to spend $1 trillion globally on cybersecurity products and services between now and 2021.[5] In the CP sector, 85 percent of companies participating in the "Cyber risk in consumer business" survey report they have increased their budgets in the past year.[6]

The cybersecurity workforce is commonly the guardian of all types of corporate information, from proprietary product formulations, patents, and company financials to the Personally Identifiable Information (PII) companies collect from their consumers.

While it's imperative that organizations take an aggressive approach to mitigating cyber risk, **it's critical for CP companies to consider increasing their cybersecurity efforts, including cybersecurity talent, now that many are using newer technologies, such as customer analytics, cloud integration, connected devices, and digital payment technology.** These technologies typically help facilitate both marketing programs and direct-to-consumers sales; they often also involve collecting PII data such as credit card information, cell phone numbers, online and off-line addresses, and birth dates.

But similar to other industries, CP companies often have a difficult time attracting, hiring, and maintaining top cybersecurity talent. Deloitte's study, "Cyber risk in consumer business," indicated that **24 percent of CP cyber executives cite lack of available talent and finding talent with the right skill set as a challenge they face.[8]**

Defining the cyber workforce

The cyber workforce is composed of roles that have an impact on an organization's ability to protect its data, systems, and operations. Examples include:

- **Those specifically focused on cybersecurity risk, governance, and operations**
- **Practitioners applying security knowledge to support the organization's mission**
- **Individuals dealing with technology or an organization's data[7]**

The difficulties of attracting cyber talent across all industries

Across all industries **the demand for cyber talent far outweighs the available talent pool.** This is made all the more compelling by employment statistics in the cybersecurity field. According to a new cybersecurity workforce study by ISACA's Cybersecurity Nexus (CSX), only 59 percent of surveyed organizations say they receive at least five applications for each cybersecurity opening, while only 13 percent receive 20 or more. In contrast, studies show most corporate job openings result in 60 to 250 applicants.[12] In this case, low unemployment has its negative consequences.

Recruitment of cybersecurity professionals tends to focus on candidates with traditional educational backgrounds with concentrations in information technology or cybersecurity, thus limiting the potential pool of cybersecurity talent in a highly competitive talent marketplace. In addition, many organizations also require security certification: Highlighting the traditional approach to recruiting talent, 7 in 10 IT professionals in the ISACA's study indicate that their organizations typically require certification for open positions.[13]

But in light of the difficulties of finding the right talent, **the ISACA study also indicates that qualifications for cybersecurity professionals are shifting:** Fifty-five percent of organizations report that practical, hands-on experience is the most important cybersecurity qualification.[14] Another study suggests that the gap in cyber talent is forcing security employers to hire more creatively, considering potential hires with nontraditional skill sets: Eighty-one percent of organizations said the skills required to be a "great" staff member had changed in the past few years.[15]

Another factor contributing to a limited talent pool of cyber talent is that women are underrepresented in the cybersecurity field. The Center for Cyber Safety and Education and the Executive Women's Forum on Information Security, Risk Management & Privacy recently completed the first-ever "2017 Global Information Security Workforce Study: Women in Cybersecurity." The study found that women make up just 11 percent of the global cybersecurity workforce. The percentage of women in the cybersecurity workforce continues to decline as cybersecurity professionals ascend the career ladder, resulting in just 5 percent of women at the executive level and 4 percent at the C-level in the cybersecurity field.[16]

- **As of July 2017, approximately 349,000 cybersecurity jobs in the US remained unfilled.[9]**

- **By 2022, the global shortfall in the information security workforce is projected to exceed 1.8 million workers.[10]**

- **Specific to CP, 49 percent of CP executives agree that cyber talent is in high demand.[11]**

The challenge of attracting cyber talent is even greater for CP companies

In addition to the challenges of finding cybersecurity talent in the general marketplace, CP companies have an added issue: Compared to their parents' generation, Millennial and future Gen Z workers who fuel the pipeline of cybersecurity professionals may not find CP companies as attractive. A recruiting expert in the CP industry posits that the many talented people coming out of business school today are more likely to pick technology or investment banking than CP companies.[17] Further, Millennials tend to be more interested in working for organizations committed to social impact programs aligned with causes meaningful to them, such as economic, environmental, and social issues of the time.[18]

Another challenge CP companies face is that Millennials tend to not be as interested in working for large companies as their parents were, preferring more entrepreneurial environments with greater challenges and personal freedoms.[19] Furthermore, tech companies also tend to be located in more appealing cities or tech hubs, which many younger, cybersecurity professionals find especially appealing.[20] For example, workforce data suggest that the shortages in tech talent have been ongoing because candidates are flocking to the four major cities for technical jobs—San Francisco, San Jose, Seattle, and Austin.[21] These concerns also surfaced during the executive interviews conducted as part of the "Cyber risk in consumer business" study, which suggested that many consumer businesses do not have the same cachet as tech companies, which tend to offer higher levels of compensation, training, and learning opportunities.

As identified in Deloitte's "Cyber risk in consumer business" study, once cyber talent has been identified and hired, there can be challenges associated with training, providing challenging learning opportunities, and risk of attrition.

The threat from employees within is also a concern for many consumer businesses. The damage done by an internal agent can be devastating depending on what information the employee has access to. Thus, managing insider threats is a cybersecurity initiative among 29 percent of the CP executives participating in the "Cyber risk in consumer business" study. In in-depth discussions, cyber executives noted that these threats appear to be more often due to employee error than malicious intent on the part of employees, but they can be as devastating as external threats.[23]

Figure 1. Challenges surveyed CP executives have with cybersecurity talent

40%
Face challenges finding and selecting the right training opportunities

29%
Feel that training opportunities are not leading-edge enough for cyber executives

17%
Fear the risk of attrition

14%
Are concerned about providing challenging learning opportunities for cybersecurity professionals

What can CP businesses do to optimize cybersecurity talent?

To help solidify their defenses against cybersecurity threats, CP companies could benefit by following the suggestions outlined in the "Cyber risk in consumer business" report on talent and taking steps to make CP organizations more attractive to the cybersecurity workforce of tomorrow.

Developing cyber talent

For cybersecurity in particular, CP companies could benefit from implementing measurable cybersecurity learning and awareness programs and supporting the daily behaviors of their associates needed to protect the organization and its people from a pervasive security breach. More specifically, this can be accomplished by:

- **Establishing a dedicated cybersecurity function** led by the CISO with skilled cybersecurity staff in place to protect business-sensitive assets, monitor security threats, and be ready to respond to breaches that may occur. The development of cybersecurity workforce strategies can be accomplished by assessing workforce needs and skill gaps; recruiting skilled talent for well-defined cybersecurity management roles; providing specialized training as needed to further enhance employee skill sets; and creating a productive, results-driven environment to retain talent.
- **Providing proactive learning and awareness** opportunities in the form of frequent, small bites of information while leveraging multiple delivery channels (such as digital, classroom-based, etc.).
- **Developing and implementing a comprehensive third-party risk program**. Often, third-party vendors are employed to fill the cyber talent gap. But in light of dependence on third-party vendors to implement advanced cybersecurity programs, it can be prudent to mandate consistent third-party governance standards and periodically conduct third-party audits.

Attracting cyber talent to the CP industry

To attract top cybersecurity talent, CP companies could benefit from a deeper commitment to training and development. Currently, security awareness and cyber risk is somewhat of a priority for many CP companies: In the "Cyber risk in consumer business survey," CP executives rated their company's maturity level only 3.7 on a 5.0 point scale.[24] Thus, increased commitment to these efforts could only be beneficial.

CP companies may want to consider offering multiple employee benefits targeted specifically to younger workers who are the lifeline of future cybersecurity programs. This may include benefits such as flexible working schedules, more casual work environments, and locations convenient to where younger workers live—for example, several major corporations in the Chicago metropolitan area have opened offices in the city after years of being located in hard-to-reach suburban areas.

Another approach CP companies may want to consider is aligning their corporate responsibility initiatives with causes Millennial workers tend to be interested in, such as the economic, environmental, and social issues of the time.[25]

In addition, CP companies may benefit from hiring cyber talent with nontraditional educations as well as focusing on women, who are underrepresented in the cybersecurity field.

To fill the cybersecurity talent gap, hiring third-party vendors is an option to help CP companies integrate newer technologies into their businesses. However, this can open new possibilities to cyber risk if relationships are not managed correctly from onboarding through frequent assessments. Deloitte's study, "Cyber risk in consumer business," indicated that frequency of third-party risk assessment is low, with only 7 percent of CP executives surveyed conducting third-party risk assessment on a quarterly basis and 34 percent on a semi-annual basis.[26]

There are also creative ways that CP companies can stimulate awareness and interest in cybersecurity. For example, the Deloitte study found that some CP companies are training their employees on how to secure their personal information as well. The rationale for this is that if employees understand the threats to them personally, they will likely be more vigilant at work. Topics addressed tend to be more basic, focusing on the fundamentals of cybersecurity, such as identity and password protection, using secure Wi-Fi networks, identifying and deleting suspicious emails, W-2 fraud, and safe use of mobile devices.

Another approach to solving the small cyber talent pool is to build interest in cybersecurity among students at a very young age. For example, recognizing the need to develop top cyber talent, China launched cybersecurity talent training nationwide in September 2016.[27] This could serve as a model for the United States and other

countries hoping to advance cyber risk management. An education official at the 4th China Internet Security Conference in August 2016 stated that the country needs at least 500,000 cybersecurity experts, but only about 8,000 such majors graduate each year. Authorities from Wuhan, capital of Central China's Hubei Province, announced plans to double the number of scholarships to attract students pursuing cybersecurity and run special recruitment for "maverick geniuses," which constitute a part of nationwide efforts to train cybersecurity talent. The Chinese government has not only established an innovative evaluation system that gives priority to practical and entrepreneurship training, but it will also offer twice the salary and research funds to the best cybersecurity experts.

Applying these principles to cyber talent in CP companies, as well as the lessons learned in the "Cyber risk in consumer business" report can help CP companies:

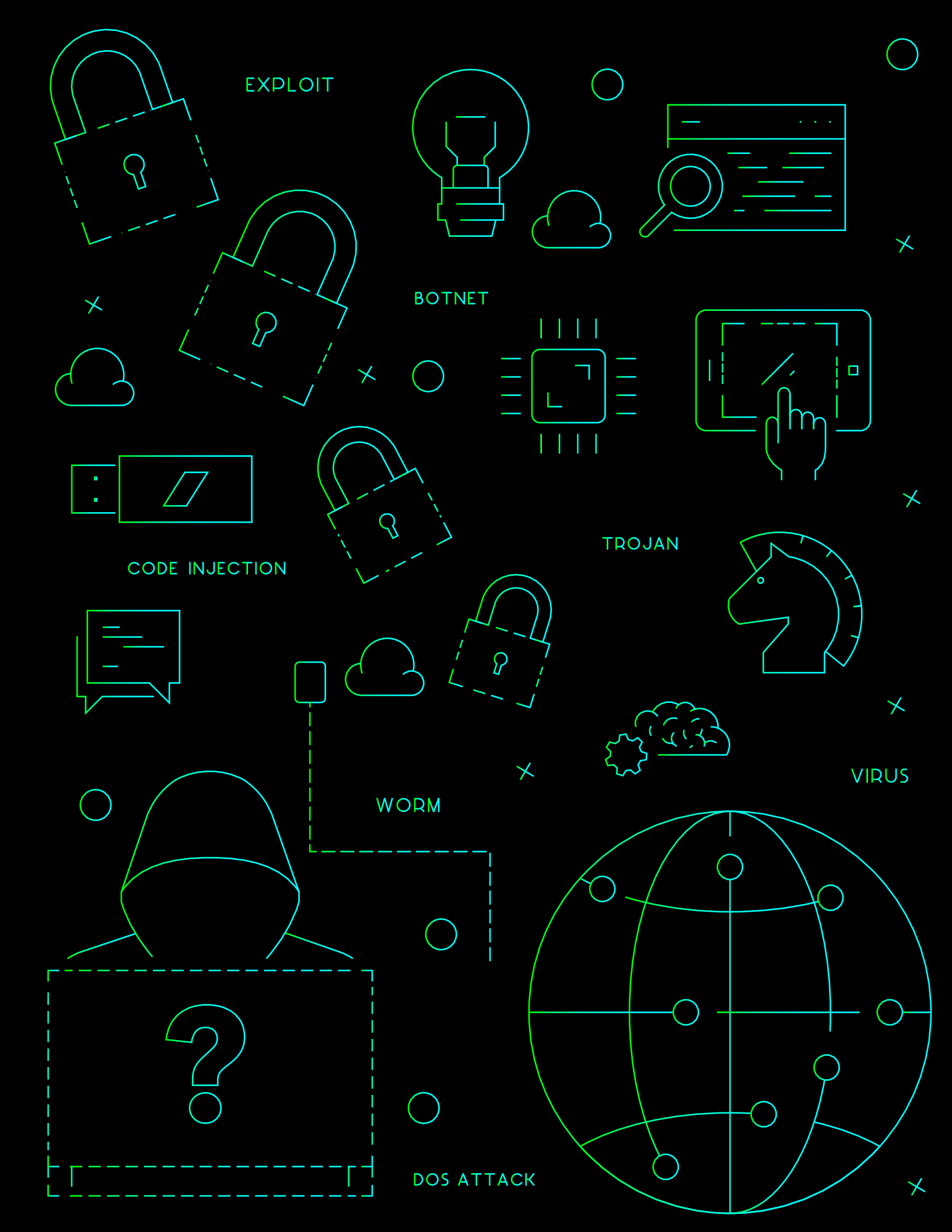
Be secure: Take a measured, risk-based approach to what is not secured and how to secure it. This includes managing cyber risks as a team and increasing preparedness by building cyber risk management strategies in the enterprise and emerging technologies as they are deployed.

Be vigilant: Monitor systems, applications, people, and the outside environment to detect incidents more effectively. This includes developing situational awareness and threat intelligence to understand harmful behavior and top risks to the organization and actively monitoring the dynamic threat landscape.

Be resilient: Be prepared for incidents and decrease their business impact by improving organizational preparedness to address cyber incidents before they escalate. This also includes capturing lessons learned, improving security controls, and returning to business as usual as quickly as possible.

Endnotes

1. Lily Hay Newman, "The Biggest Cybersecurity Disasters of 2017 So Far," *Wired*, https://www.wired.com/story/2017-biggest-hacks-so-far/, last modified August 1, 2017.
2. Sean Peasley, Kiran Mantha, Vikram Rao, Curt Fedder, and Marcello Gasdia, "Cyber risk in consumer business: Consumer businesses discuss the six main cyber risk challenges they face today," Deloitte University Press (now Deloitte Insights), June 15, 2017, https://www2.deloitte.com/insights/us/en/industry/retail-distribution/cyber-risk-management-in-consumer-business.html, accessed January 2018; and Barb Renner and Curt Fedder, "Why CMOs should care about cyber risk," Deloitte LLP, January 10, 2018, https://www2.deloitte.com/us/en/pages/consumer-business/articles/why-consumer-products-cmos-should-care-about-cyber-risk.html, accessed January 11, 2018.
3. Peasley, Mantha, Rao, Fedder, and Gasdia, "Cyber risk in consumer business."
4. Cybersecurity Ventures, "Hackerpocalypse: A cybercrime revelation," http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, accessed April 2, 2017.
5. Ibid.
6. Peasley, Mantha, Rao, Fedder, and Gasdia, "Cyber risk in consumer business."
7. Sharon Chand and Elaine Loo, "The cyber talent gap: New considerations and strategies," recorded August 23, 2017. https://www2.deloitte.com/us/en/pages/dbriefs-webcasts/events/august/2017/dbriefs-cyber-talent-gap-new-considerations-and-strategies.html, posted August 24, 2017.
8. Peasley, Mantha, Rao, Fedder, and Gasdia, "Cyber risk in consumer business."
9. Cyber Seek, "Cybersecurity Supply/Demand Heat Map," http://cyberseek.org/heatmap.html, last updated July 22, 2017.
10. "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," (ISC)2, March 2017, https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf, accessed January 2018.
11. Ibid.
12. ISACA, "Cybersecurity Skills Gap Leaves 1 in 4 Organizations Exposed for Six Months or Longer," http://www.isaca.org/About-ISACA/Press-room/News-Releases/2017/Pages/Survey-Cyber-Security-Skills-Gap-Leaves-1-in-4-Organizations-Exposed-for-Six-Months-or-Longer.aspx, accessed January 2018.
13. Ibid.
14. Ibid.
15. Ryan Golden, "Cyber talent gaps force IT security employers to hire creatively," *HR Dive*, http://www.hrdive.com/news/cyber-talent-gaps-force-it-security-employers-to-hire-creatively/504966/, last modified September 14, 2017.
16. "Global Information Workforce Study," (ISC)2, 2016.
17. Elaine Watson, "Recruitment Focus: 'The consumer products industry is facing a serious talent shortage,' " FOODnavigator-usa.com, https://www.foodnavigator-usa.com/Article/2015/04/20/CPG-industry-facing-a-serious-talent-shortage-recruiter, last updated April 20, 2015.
18. Claire Hassett and Christine Selph, "The Deloitte Millennial Survey 2017," Deloitte Touche Tohmatsu Limited, https://www2.deloitte.com/global/en/pages/about-deloitte/articles/millennialsurvey.html, accessed January 2018.
19. Watson, "Recruitment Focus: 'The consumer products industry is facing a serious talent shortage.' "
20. Peasley, Mantha, Rao, Fedder, and Gasdia, "Cyber risk in consumer business."
21. Tess Taylor, "How to recruit hard-to-find tech talent," *HR Dive*, http://www.hrdive.com/news/how-to-recruit-hard-to-find-tech-talent/425613/, last modified September 1, 2016.
22. Peasley, Mantha, Rao, Fedder, and Gasdia, "Cyber risk in consumer business."
23. Ibid.
24. Ibid.
25. Hassett and Selph, "The Deloitte Millennial Survey 2017."
26. Peasley, Mantha, Rao, Fedder, and Gasdia, "Cyber Risk in consumer business."
27. Cao Siqi, "China launches cybersecurity talent training nationwide," *Global Times*, http://www.globaltimes.cn/content/1007158.shtml, last modified September 20, 2016.


EXPLOIT
BOTNET
CODE INJECTION
TROJAN
WORM
VIRUS
DOS ATTACK

Contact

Barb Renner
Vice Chairman & US Leader
Consumer Products
Deloitte LLP
brenner@deloitte.com

Acknowledgments

We wish to thank:

Curt Fedder, senior manager, Deloitte Services LP
Jagadish Upadhyaya, assistant manager, Deloitte Support Services India Pvt. Ltd.
Shweta Joshi, senior analyst, Deloitte Support Services India Pvt. Ltd.,
and others who contributed their ideas and insights to this paper.

Deloitte.

Deloitte Center *for*
Industry Insights

About the Deloitte Center for Industry Insights
The Deloitte Center for Industry Insights (the Center) provides premier insights based on primary research on the most prevalent issues facing the consumer business and manufacturing industries to help companies run effectively and achieve superior business results. The Center is associated with the Deloitte US firms' Consumer & Industrial Products practice, which benefits from the insights of over 12,000 multi-disciplined professionals with a wide array of deep, hands-on industry experience.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.