AN A.S. PRATT PUBLICATION
JUNE 2019
VOL. 5 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 5 | JUNE 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call
Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [137] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

EU Cyber Threat Landscape and Outlook: What You Should Know About the ENISA Report

Diletta De Cicco and Charles-Albert Helleputte*

This article discusses some of the European Union Agency for Network and Information Security's 2018 Threat Landscape Report and the Agency's recommendations for businesses to increase resilience and foster improved cybersecurity in 2019.

The landscape for cyberattacks is constantly evolving. Attacks are becoming more global and sophisticated, and 2019 is poised to continue this trend toward increasing complexity. This article highlights: (i) the main aspects of the threat landscape identified by the European Union Agency for Network and Information Security ("ENISA") in its 2018 Threat Landscape Report[1] (the "Report") published on January 28, 2019, and (ii) the recommendations from ENISA for businesses to increase resilience and foster improved cybersecurity in 2019. Set up in 2004, ENISA is contributing to a high level of network and information security ("NIS") within the European Union and working to develop a culture of NIS, and raise awareness, in society. Its yearly edition of the Report contributes to the identification of the cyber threat landscape and supports the development and implementation of the European Union's policy on matters relating to NIS.

CYBER THREAT LANDSCAPE IN 2018: MORE OF THE SAME AND ONE NEW JOINER

The Report identifies the top 15 cybersecurity threats in Europe. The top four threats remain unchanged compared to the previous year:

(1) malware;

(2) web-based attacks;

(3) web-application attacks; and

(4) targeted forms of phishing (in that order).

* Diletta De Cicco is an associate practicing in Mayer Brown's Global Cybersecurity and Data Privacy team. Charles-Albert Helleputte is a partner in the firm's Global Cybersecurity and Data Privacy team and the head of the firm's Cybersecurity and Data Privacy practice in Brussels. The authors may be reached at ddecicco@mayerbrown.com and chelleputte@mayerbrown.com, respectively.

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

Meanwhile, denial of service ("DoS") botnets and data breaches increased in 2018. The Report also found a new threat: "cryptojacking." This article discusses some of the Report's findings.

- DoS attacks, and especially distributed DoS ("DDoS") attacks, are an impactful threat in the cyber landscape and have been used to target businesses across economic sectors. Defending against this type of threat (notably by hiring dedicated vendors) has become a central challenge for the private sector with financial services, e-commerce companies, cloud providers, and governments devoting significant resources to the issue.[2] Research suggests that the number of DDoS activities is on the rise (a 16-percent increase in summer 2018 when compared to the same period in 2017).[3] Although law enforcement activities have challenged this breed of malicious cyber activity, the Report noted that the increase in the number of connected services globally and their dependency on the internet of things ("IoT") increase the threat of DoS and other types of attacks. As connectivity grows, such attacks have the potential to cause systemic failure for businesses and critical systems (e.g., in connected hospitals and related services).
- The Report noted that, during 2018, botnets were active and used to advance various malicious activities. For example, the Report revealed that 88 percent of spam was found to have originated from botnets and new botnets have been developed around IoT, social media and online advertisements. The Mirai malware technique (and source code) inspired criminals to build even more sophisticated IoT botnets (Tori-bot, a prominent type of botnet identified in the Report, has six persistency techniques targeting multiple architectures.)
- The Report noted that data breaches (incidents leading to the alteration, compromise, or loss of data) have affected significantly more records in 2018,[4] with the average cost of breach increasing by 6.4 percent. The introduction of a more comprehensive data breach framework in the European Union (since the entry into force of the General Data Protection Regulation) could explain some of that increase. Social media platforms account for a majority (56 percent) of reported breaches, and some industry sectors (e.g., healthcare, 27 percent) have been particularly vulnerable. The Report found that 48 percent of breaches were caused by external attackers first, while human

[2] *See* the Arbor network report, https://pages.arbornetworks.com/rs/082-kna-087/images/12th_worldwide_infrastructure_security_report.pdf.

[3] *See* https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf.

[4] 4.5 billion data files were breached worldwide in the first half of 2018, up from 2.7 billion in the same period of 2017, according to the data breach index cited in the Report.

error and negligence, along with technical error, accounted for 27 percent and 25 percent, respectively.

- According to the Report, 2018 was the year of cryptojacking, a phenomenon appearing among the top 15 threats for the first time. Cryptojackers use the victim's computer power to "mine" cryptocurrencies, such as Bitcoin or Monero, without the victim's consent. Higher profits have driven cybercriminals to focus on cryptojacking. The implementation of content filtering that screens out suspected cryptojacking software in emails and employs regular security audits should, according to the Report, help to detect anomalies in the usage of computer power linked to cryptojacking.

IN 2019, ORGANIZATIONS SHOULD PURSUE A CYBERSECURITY STRATEGY

Throughout the Report, ENISA identified specific measures that could be adopted in the business context to minimize risks to cybersecurity. According to the Report, recommended steps in the development of a cybersecurity strategy include the following:

- *Estimate risks from cyber threats, or "know your enemy" (and yourself).* Businesses should assess the potential impacts of a successful cyberattack on their assets and customer base and adopt the required security measures. Risk assessment should take into account the evolution of cyber threats, particularly the growing focus on automated attacks and attacks on mobile devices and IoT.
- *Define cyber threat intelligence* ("CTI") *processes.* Collection and analysis of CTI contributes to a better understanding of the motives and techniques used to conduct a cyberattack (and the ability to anticipate potential damage).
- *Share CTI with other stakeholders.* Sharing CTI can help facilitate the identification of common threats, as well as best practices and effective security measures (eventually at a sector-specific level). Existing CTI networks should be enlarged, and the volume of CTI shared should be increased.
- *Consider supply chain threats.* In complex product development processes, threats affecting different levels of the supply chain can have a cascading effect that ultimately impacts the end user. Coordinated action at a sector-specific level should ensure a common approach to these systemic threats. In addition, relying on certification at every stage of the supply chain may help to facilitate end-to-end security.

In all of these aspects, the role of ENISA is set to increase in 2019 following the adoption of the EU Cybersecurity Act. The Cybersecurity Act paves the way for EU cybersecurity certification schemes for ICT products (i.e., hardware and software

elements of network and information systems); services (i.e., services involved in transmitting, storing, retrieving or processing information via network and information systems); and processes (i.e., sets of activities performed to design, develop, deliver and maintain ICT products and services). Since 2019 is the first full year since the adoption of the NIS framework by EU member states, cybersecurity awareness will be a key consideration for businesses operating in the European Union.

CONCLUSION

Cybersecurity is likely to stand among the most significant challenges that multinational businesses must address in 2019. Businesses will benefit from continuing to refine their cyber risk management and data privacy compliance programs to address the evolving EU cyber regulatory landscape.