Data and Privacy: 2018-2019 Outlook

2018 has been a landmark year for data protection, and in 2019, data privacy concerns along with global information security spending will continue to rise in excess of $124B, according to Gartner. Security leaders continue to assist organizations in utilizing technology platforms securely, with an aim to stay competitive and drive business growth.

This e-book will explore where the world - and the US specifically - stands with data protection in 2018 and what we have in store for this very important topic in 2019.

165 HALSEY STREET

Contents

2018: The Year Data Privacy Got Real

2018 has been a landmark year for data protection, and in 2019, data privacy concerns along with global information security spending will continue to rise in excess of $124B, according to Gartner. Security leaders continue to assist organizations in utilizing technology platforms securely, with an aim to stay competitive and drive business growth. Additionally, 2018 was the year of the new General Data Protection Regulation (GDPR), which is presently leading the way in its approach to data protection and privacy in the digital age. As technology continues to develop at a rapid pace, how can companies keep up to ensure security and data privacy?

This e-book will review the latest stats on global data privacy, what's ahead for new laws and regulations, how companies can prevent data breaches and more.

GDPR is Here – Now What?

According to "*The Race to GDPR: A Study of Companies in the United States & Europe*" survey conducted by McDermott Will & Emery, 60% of respondents said GDPR has significantly changed their organizations' workflows for collecting, using, and protecting personal information.
.

General Data Protection Regulation (GDPR) enforcement, began officially on May 25, 2018.

GDPR is designed to not only standardize privacy practices across the EU, but to influence how countries outside the EU design their own legislation around data protection and privacy. The GDPR applies to data captured and processed by EU-based businesses, but also to any organization outside the EU that processes personal data about EU customers in connection with offering goods or services to them. The penalties for GDPR noncompliance can be quite significant – with fines up to €20 million or four percent of total worldwide revenue the previous year, whichever is greater.

Although GDPR is now in place, and technology continues to develop at a rapid pace, the new EU data protection framework remains incomplete, and revised data protection rules are still urgently needed. Additionally, according to new research (August 2018), EU businesses are still struggling to become compliant with GDPR, risking huge fines in the process. For US businesses particularly, they must provide Privacy Shield-Compliance Privacy Policy statements as part of the self-certification process, or self-certifying organizations can choose to prove compliance through an independent party or a self-assessment. However, if the US continues to stall in efforts around data privacy, global partners may force US businesses to adopt GDPR compliance in its totality. Contract terms will no longer be able to accept Privacy Shield assurances as an alternative to full compliance. A US company expanding its services and technology to the EU market then needs to become GDPR compliant as it scales.

GDPR is Here – Now What? (Cont'd)

Recommended Next Steps for U.S. Businesses

Courtesy of Jaymie Scotto & Associates (JSA)

- Determine whether or not you are using email addresses from the EU. If the email has an .eu .de .nl .be .es .uk .it .se .ch .pl at extension, that's a pretty good sign. Other than that you may need to use the IP address to help you locate the origin.
- Prepare for a new opt-in campaign for your existing EU customers. Even if you previously obtained permission to use their email address, you will need to solicit permission from them once again.
- Review any requests for email addresses, including pop-up windows and sign-up forms, to make sure the language is clear and specific, and covers all the reasons for using that address.
- Keep a record of all individual permissions to use their email address and be prepared to present the consents if asked.
- Take steps to protect against potential breaches in security. Review your current data storage and security practices to see if additional measures should be added.

The information above is generalized and not legal advice. To mitigate GDPR risks, 165 Halsey Street recommends that your organization is working with an experienced information sharing and analysis organization (ISAO).

Stats on Global Data Privacy

Quick cybersecurity stats:

- Ransomware attacks are growing more than 350% annually.
- IoT attacks were up 600% in 2017.
- Approximately 24,000 malicious mobile apps are blocked every day.
- The average cost of a malware attack on a company is $2.4 million. (Accenture)
- Damage related to cybercrime is projected to hit $6 trillion annually by 2021.

According to leading research firm, Gartner:

- Worldwide spending on information security products and services will reach over $114 billion in 2018, an increase of 12.4% from last year, according to the latest forecast from leading research firm Gartner. The firm is also forecasting that the market will to grow 8.7% to $124 billion in 2019.
- At least 30% of organizations will spend on GDPR-related consulting and implementation services through 2019.
- Risk management and privacy concerns as part of digital transformation initiatives will drive additional security service spending through 2020 for over 40% of organizations.
- Cloud-delivered security is becoming the top preferred delivery model for an array of technologies.

"With information security spending expected to reach upwards towards $124b in 2019, the topic of cybersecurity remains one of the hottest in the tech and telecom industries today. A critical issue that spans the world, there remain several challenges, including a shortage of skills and lack of total control. Fortunately, with the focus so strongly on cybersecurity, leaders continue to take the reins in exploring the technologies and techniques needed to successfully confront cyberattacks." **--Joseph Simone, President at Tishman Real Estate Services for 165 Halsey Street.**

What’s Ahead for More Privacy Laws?

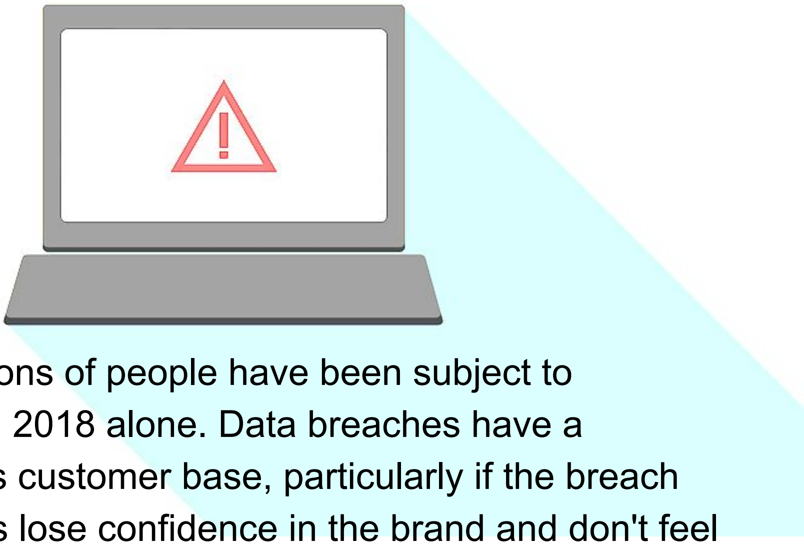
As of March 2018, in response to the EU’s newly enacted GDPR, all 50 U.S. states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted breach notification laws requiring businesses to notify consumers if their personal information is compromised. These new and amended state data breach laws further define personal information and specifically mandate that certain information security requirements are implemented.

In California and Vermont specifically, the two states go beyond breach notification and require companies to make significant changes in their data processing operations. In other parts of the globe, the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System has been gaining momentum both in terms of the number of countries that have joined and the number of industry associations and companies supporting the initiative. The system was designed to facilitate cross border data flows and raise the level of privacy protection for consumers in the APEC region. Currently, six countries (Canada, Mexico, Japan, the U.S., South Korea, and Singapore) are participating or in process of joining the system, and others (Australia, Philippines and Chinese Taipei) have noted their interest in joining also.

As a whole, the expanding global privacy and security community will need to address the complicated data security issues in the coming year. The issues include GDPR implementation and related data transfer rules for the EU and globally, as well as practical and operational issues that involve putting best practices for new data and technology into place. Data professionals are strongly needed to become “effective stewards of company data, with appropriate consideration of individual privacy and appropriate business goals,” and companies must focus on the need to manage individual data, while dealing with the onslaught of legislative and regulatory overlaps and the need for effective integration of privacy and security controls.

It’s a lot to deal with, folks - and resources are available. Talk to the data security professionals at 165 Halsey Street to learn more.

How Companies Can Prevent Data Breaches



From Facebook to T-Mobile, hundreds of millions of people have been subject to compromised records due to data breaches in 2018 alone. Data breaches have a considerable, negative impact on a company's customer base, particularly if the breach involves sensitive data. Not only do customers lose confidence in the brand and don't feel that their data is secure, but data breaches puts off new potential customers as well. How can companies best prevent costly data breaches?

1. Incorporate a cybersecurity specialist into the team.
2. Keep all business and personal accounts separate, and encrypt all data.
3. Continue to build awareness. Strengthen passwords and require both a two-step identification process and good antivirus programs.

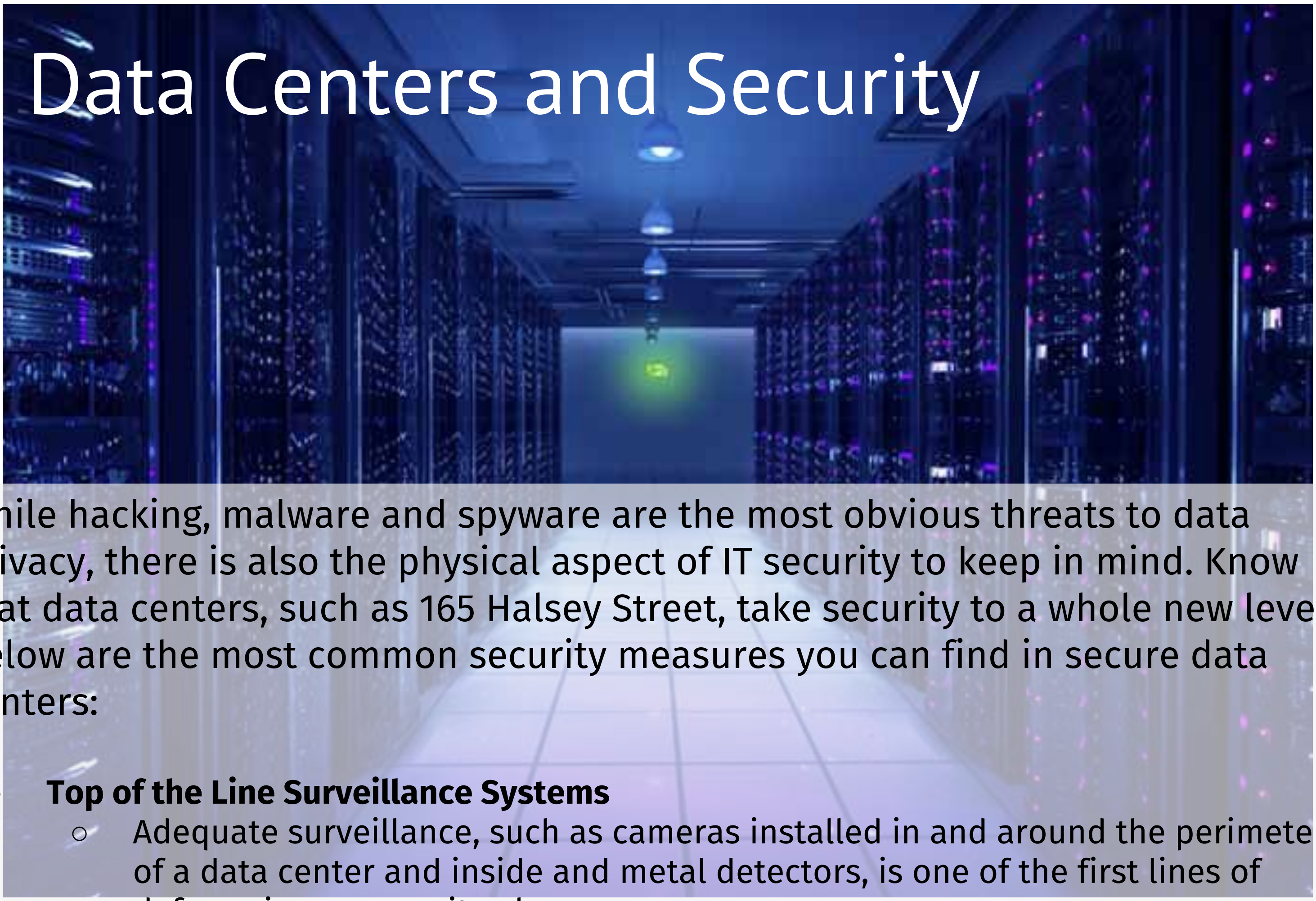
4. Educate the workforce. Train employees on how to encrypt data, generate strong passwords and properly file and store data. Limit employee access to websites outside the scope of their regular duties, and inform them of malware dangers and how to avoid.

5. Solidify and implement a process to secure all data. All companies need to have a sense of urgency to control data by establishing a proper process and training.

6. Ensure and enforce restrictive data permissions. A lot of breaches occur due to an employee breach. Companies should continuously ensure that employees have limited access only to the information that is vital to their jobs.

7. Check the Financial Industry Regulatory Authority (FINRA) cybersecurity checklist, which offers companies a useful guide on taking existing security measures and course of action to take if breaches take place. Visit http://www.finra.org/industry/cybersecurity for more info.

Data Centers and Security

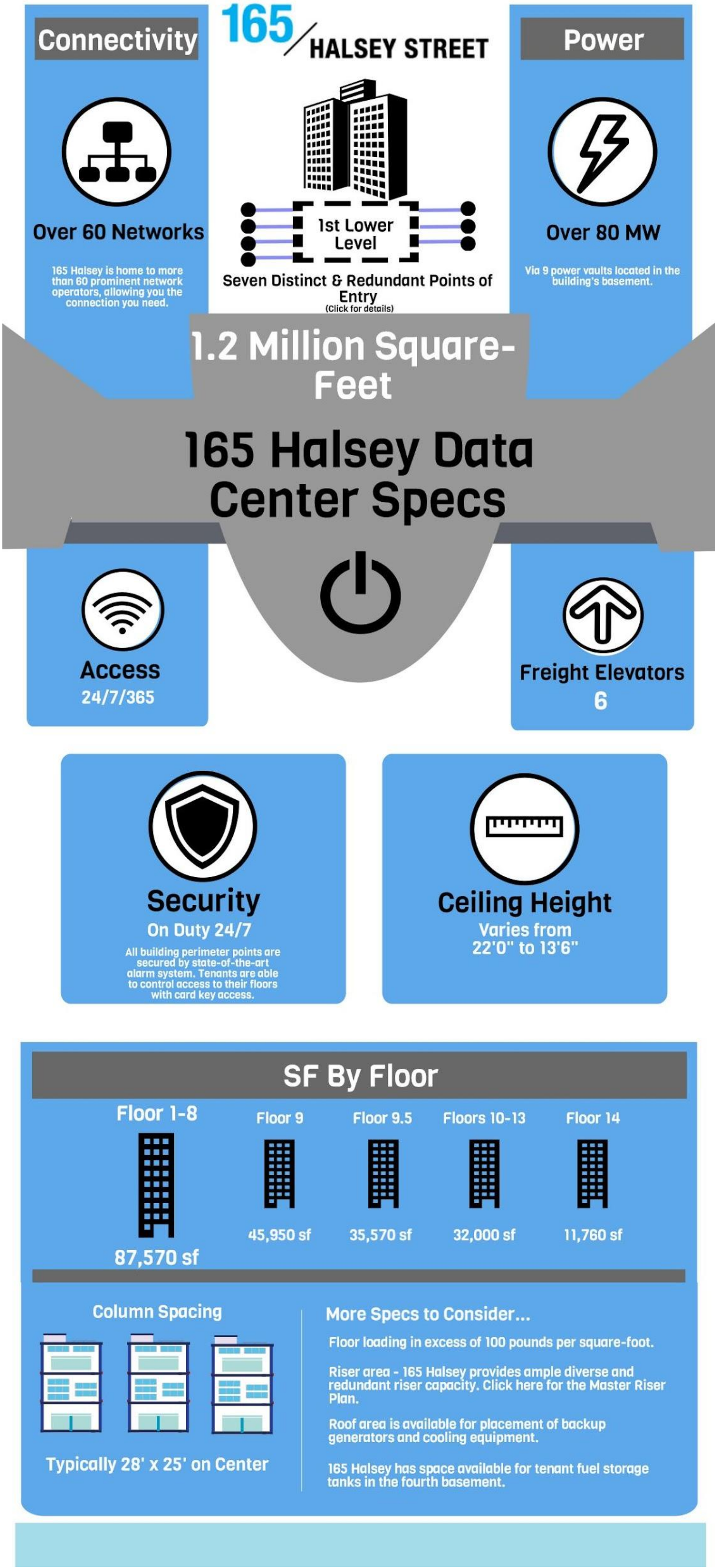


While hacking, malware and spyware are the most obvious threats to data privacy, there is also the physical aspect of IT security to keep in mind. Know that data centers, such as 165 Halsey Street, take security to a whole new level. Below are the most common security measures you can find in secure data centers:

- **Top of the Line Surveillance Systems**
  - Adequate surveillance, such as cameras installed in and around the perimeter of a data center and inside and metal detectors, is one of the first lines of defense in any security plan.
- **Security Guards**
- **Strategic Building Design**
  - Secure data centers are built strictly for the purpose of housing IT infrastructure and are designed accordingly. Interiors are designed to separate the main data center area from any other rooms, such as an entrance lobby, breakroom or restrooms. Security increases the closer you get to the center of the data center, requiring multiple forms of identification or access control.
- **Access Control**
  - Only authorized personnel are allowed in these secured areas, where the servers, routers and other equipment live. To prevent unauthorized individuals from accessing or tampering customer data or installing malicious hardware, data centers employ a wide array of access controls throughout a data center. Mantraps are also often utilized to limit access to authorized individuals and prevent criminals from tailgating, the practice of following someone closely to gain unauthorized entry to a secure area. A mantrap is typically a set of two doors with an airlock in the middle, and both doors of a mantrap require authentication, such as a keycard or biometric lock.

There are many additional countermeasures employed by data centers. Check with your data center specifically on all security measures utilized.

Why 165 Halsey Street?



165/HALSEY STREET

Connectivity

Over 60 Networks

165 Halsey is home to more than 60 prominent network operators, allowing you the connection you need.

1st Lower Level

Seven Distinct & Redundant Points of Entry
(Click for details)

Power

Over 80 MW

Via 9 power vaults located in the building's basement.

1.2 Million Square-Feet

165 Halsey Data Center Specs

Access
24/7/365

Freight Elevators
6

Security
On Duty 24/7
All building perimeter points are secured by state-of-the-art alarm system. Tenants are able to control access to their floors with card key access.

Ceiling Height
Varies from 22'0" to 13'6"

SF By Floor

Floor 1-8	Floor 9	Floor 9.5	Floors 10-13	Floor 14
87,570 sf	45,950 sf	35,570 sf	32,000 sf	11,760 sf

Column Spacing

Typically 28' x 25' on Center

More Specs to Consider...

Floor loading in excess of 100 pounds per square-foot.

Riser area - 165 Halsey provides ample diverse and redundant riser capacity. Click here for the Master Riser Plan.

Roof area is available for placement of backup generators and cooling equipment.

165 Halsey has space available for tenant fuel storage tanks in the fourth basement.

165 Halsey Street is a dedicated 1.2M sf data center/colocation/telecom carrier hotel with over 80 MW of power. The building has been operating a carrier neutral colocation business for more than 15 years, and presently spans over 180, 000 square feet with **no MRC cross connect fees** and direct access to over 60 networks.

Located just 13 miles from Manhattan, 165 Halsey Street is independently owned and operated and SSAE 16-certified. With **165 Halsey Colocation**, there are no monthly recurring cross connect fees between customers, allowing safe, convenient and affordable interconnection.

If looking to colocate or build out in 2017 or the year ahead, look no further than 165 Halsey Street.

✓Prime Location – 13 mi from Manhattan
✓80 MW Power
✓Affordable Colocation; No Cross Connect Fees
✓Disaster Recovery Planning
✓Solid Communications Infrastructure: Access to Over 60 Networks
✓Built Data Center Space
✓Vacant Space

CONTACT US

Telecom and Data Center Building
165 Halsey Street, Newark, NJ 07102
http://www.165halsey.com

Leasing & Licensing
Joseph Simone
212-399-3633
simone@tishman.com

James Fitzgerald
212-708-6741
jfitzgerald@tishman.com

Colocation
Joe Panella, Manager
973-951-2358
jpanella@165halsey.com

@165Halsey

165 Halsey

ONLINE SOURCES

Barkly
https://blog.barkly.com/biggest-data-breaches-2018-so-far

Big Law Business
https://biglawbusiness.com/the-top-ten-privacy-and-data-security-developments-to-watch-in-2018/

Data Protection Report
https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/

EDPS.Europe.eu
https://edps.europa.eu/press-publications/press-news/press-releases/2018/data-protection-and-privacy-2018-going-beyond-gdpr_en

Forbes
https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#5475c0bb7112

https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7d42882e60ba

https://www.forbes.com/sites/forbesfinancecouncil/2018/03/08/how-to-protect-your-business-from-a-data-breach-seven-key-steps/#14f0575f6b68

HelpNet Security
https://www.helpnetsecurity.com/2018/08/27/privacy-shield/

ITPro Portal
https://www.itproportal.com/news/gdpr-what-businesses-need-to-know/

JSA
https://www.jsa.net/blog/gdpr-goes-into-effect-this-month-is-your-company-ready/31115/

McDermott Will & Emery
https://www.mwe.com/en/thought-leadership/publications/2018/04/mcdermott-ponemon-institute-gdpr

MarketWatch
https://www.marketwatch.com/press-release/gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019-2018-08-22

Varonis
https://blog.varonis.com/cybersecurity-statistics/