Data Breach Industry Forecast **2018**

By Experian Data Breach Resolution • 2018 Edition

Executive summary

Today's organizations face a cybersecurity landscape more difficult to navigate than ever before. As our world grows more interconnected and technology-dependent, cybercriminals are becoming more sophisticated in their attacks and are keeping pace with our efforts to thwart them. The motivations behind cyberattacks have also expanded, making it increasingly difficult to predict and identify potential threats. With large-scale data breaches making the headlines in 2017, organizations must be proactive, not reactive, in the face of looming cyber threats.

Every day, the line between cyber threats and physical threats grows thinner — blurring the distinction between attacks on networks and attacks on our physical world. From the rise of ransomware to politically motivated data leaks, this year further established cybersecurity as one of the most significant issues impacting international security and political and economic stability.

Experian Data Breach Resolution outlines five predictions for the data breach industry in 2018. The fifth edition of the *Data Breach Industry Forecast* report sheds light on emerging trends that companies should prepare for in the new year. We've included a new section that revisits previous predictions, as some of the trends highlighted as far back as the inaugural 2014 issue are still relevant today.

Our predictions are rooted in Experian's history of helping companies navigate more than 18,000 breaches over the last decade.

Based on our experience, the top data breach trends of 2018 include the following:

» The United States may experience its first large-scale attack on critical infrastructure, causing chaos for governments, companies and private citizens.

» Failure to comply with new European Union regulations will result in large penalties for U.S. companies.

» Perpetrators of cyberattacks will continue to zero in on governments, which could lead to a shift in world power.

» Attackers will use artificial intelligence (AI) to render traditional multifactor authentication methods useless.

» Vulnerabilities in internet of things (IoT) devices will create mass confusion, leading to new security regulations.

2018 predictions

Cyberattacks that target and infiltrate critical infrastructure are very real and some have already proven successful. For the United States, it's not a matter of if, but when.

1 The United States may experience its first large-scale attack on critical infrastructure, causing chaos for governments, companies and private citizens.

In 2015, hackers hit Ukraine's power grid, leaving 225,000 people without power in the dead of winter. Just one year later, Russian hackers targeted a transmission-level substation, causing a blackout in part of the capital, Kiev. From 2015 to 2016, criminals used the SWIFT[1] global banking system to launch a string of cyberattacks, stealing millions of dollars.[2]

Cybercriminals are turning their attention to critical infrastructure as potential targets. In fact, 40 percent[3] of industrial enterprises faced cyberattacks in the second half of 2016.

More recently, the UK's energy sector was targeted and likely compromised by foreign state-sponsored hackers.[4] This attack occurred within days of similar instances in both Ireland and the United States, prompting concerns about a widespread campaign to probe energy suppliers for weaknesses and to steal credentials for future attacks.

The National Infrastructure Advisory Council (NIAC) has warned that the U.S. government and private sector are failing to defend critical systems from aggressive cyberattacks.[5] Despite reports of numerous attacks on nuclear power plants across the U.S., government officials have yet to take widespread proactive measures.

Threats may continue to increase in 2018 as hackers look to create chaos and confusion, targeting highly connected U.S. infrastructure.

The takeaway

Public and private sector organizations need to ensure that they are using the most robust technology available to thwart an attack — going beyond traditional cybersecurity and adding fail-safes to ensure continued operation. Additionally, organizations should update and practice their incident response plan, incorporating cyber threats with real-world implications.

2018 predictions

With the new EU regulation's scheduled enforcement date of May 25, 2018, any U.S. company that fails to comply with the General Data Protection Regulation (GDPR) may face severe repercussions.

2 Failure to comply with new EU regulations will result in large penalties for U.S. companies.

In 2016, after four years of preparation and debate, the EU parliament passed the GDPR[6], giving companies more than a year to prepare for one of the most extensive overhauls to data protection rights in recent memory. As this grace period comes to a close, very few businesses are ready, let alone aware of what the GDPR entails or its far-reaching implications.

The GDPR lays out strict requirements on how companies should process, store and secure the personal data of EU citizens. These conditions apply to any business around the world that handles data on EU residents, including permanent residents, visitors and expatriates.

Among the many organizational and technological process requirements, organizations must be ready to justify their reasons for obtaining every piece of data pertaining to an EU citizen. Companies must not only be transparent about how they will use the data at the time of collection, but also prove that they have the adequate data security measures in place to protect information. But perhaps one of the most significant concerns for organizations is the massive fines for noncompliance.

Uncertainty remains regarding how, and under what circumstances, data regulators will issue fines. Some have stipulated that regulators will send a clear message from the beginning by making an example of companies for noncompliance. Since the European Data Protection Board (EDPB) has yet to release any guidelines on fines, the first few cases will likely set a precedent.

The GDPR dictates that infringements can result in either fines up to €20 million (approximately $23.6 million) or 4 percent of the company's total worldwide annual turnover during the preceding financial year, depending on which is greater. Despite the potential of exorbitant fines, however, Experian Data Breach Resolution and the Ponemon Institute found that only 9 percent of U.S. multinational companies have prepared for the new requirements.[7] Additionally, more than half reported that they didn't know how to become GDPR-compliant.

Many U.S. based companies also fail to recognize that they don't have to do business in the EU to fall under the GDPR. Bottom line: If a company has any information on EU subjects, it must comply with the GDPR's rules. While there isn't an official partnership established between the U.S. and EU law enforcement agencies specific to the GDPR, U.S. authorities can help EU regulators identify and fine any U.S. company in violation of GDPR requirements.

U.S. companies that underestimate the magnitude of the GDPR, or fail to take the EU's repercussions seriously, risk more than just financial hits. Inadequate security may also cause a blow to the company's reputation.

The takeaway

The requirements outlined in the GDPR include some of the best practices companies should already have in place, including a data protection officer, a formalized breach response plan and systems to ensure data is accounted for at all times. With much uncertainty regarding GDPR fines, businesses need to invest time and resources into researching the new regulations and how they will impact their process for obtaining and securing data belonging to EU citizens.

2018 predictions

Nation-state cyberattacks are becoming far more common and politically motivated.

3 Perpetrators of cyberattacks will continue to zero in on governments, which could lead to a shift in world power.

The 2016 attacks against the U.S. Democratic Party and subsequent leaks of stolen information reflect a growing trend toward highly publicized, overt efforts to destabilize and disrupt organizations and countries.

We may continue to see hostile nations employing a combination of digital tactics (infiltrating computers, destroying files with malware or ransomware and distributing false information through social media platforms) to impact not only governments but global businesses. Companies with international reach should consider these threats in their overall response plans.

As details surrounding the 2016 election continue to materialize, it becomes apparent how challenging it is to link hackers to governments, making cyberattacks potent and dangerous weapons.

The cyberattacks perpetrated on the British[8] and Scottish[9] parliaments in June 2017 offer further warning signs. Governments may also see increased threats to compromise official, classified information relating to or coming directly from heads of state. With major elections on the horizon in the U.S. and the EU in 2018, we could see further attempts by foreign governments to disrupt and discredit democratic processes.

Technology and digitization are changing the way countries operate and defend themselves. As enemy forces barricade themselves behind screens and conflicts move to invisible battlefields, traditional rules of engagement become harder to define.

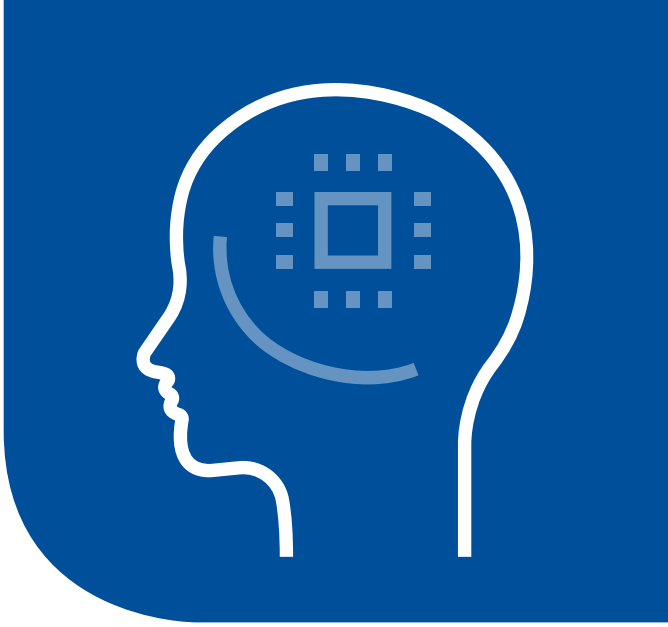
We could also see more attempts to hack into election and voting systems.[10] Fortunately, state election boards are taking steps to mitigate these risks, but without a unified effort from the federal level, the U.S. election system remains vulnerable.[11]

The takeaway

In 2016 and 2017, we witnessed the realities of nation-state cyberattacks. Moving into 2018, it's critical that governments take additional steps to protect elections and other government processes. Given the current geopolitical environment, the private sector must also take precautions to shore up data and create strategies for global business continuity in the face of data breaches.

2018 predictions

While artificial intelligence (AI) brings many benefits, widespread adoption may also lead to more effective and dangerous cyberattacks.



4 Attackers will use artificial intelligence to render traditional multifactor authentication methods useless.

There has been a growing call from the security community for companies to move away from traditional login credentials (username and password) and adopt more secure AI-based multifactor authentication methods.[12] With hacking techniques becoming increasingly sophisticated, nontraditional authentication methods will become essential to help secure accounts in 2018 and beyond.

Banks and other institutions entrusted with personally identifiable information (PII) are making strides in authentication security — leveraging AI, biometrics, behavioral patterns and distinctive user characteristics to provide more secure verification. However, AI accessibility presents a double-edged sword — while the technology can improve protection, it can also advance hacking techniques.[13]

With the potential to perfect coding and rid systems of flaws, AI opens up a world of possibilities for technology and security. However, cybercriminals can take advantage of those same capabilities to scan software to identify and exploit unknown weaknesses. AI can do this with machine efficiency. Hacks that were once time-consuming to develop will become readily available commodities.

With the role of AI expanding, 2018 will bring the first AI-enhanced cyberattack and automation will make complex attacks faster and more destructive. Imagine if hackers could take over self-driving cars or replicate biometrics to access PII. While designed to make our lives easier, these capabilities also allow hackers to carry out targeted attacks against organizations and individuals.

The takeaway

Companies should stay updated and aware of the security technology available to protect PII. While multifactor authentication is an important first step, organizations must also consider the AI platforms they are using and ensure that security providers use patented technology to keep hackers out.

2018 predictions

In 2015, we predicted that the spread of the IoT would bring a fresh breach surface for cybercriminals. We removed this prediction after no notable breach occurred at the time, but this move was premature.

5 Vulnerabilities in internet of things (IoT) devices will create mass confusion, leading to new security regulations.

As IoT devices have dropped in price, they have also become more accessible to the wider market.[14] The development of smart devices shows no signs of slowing down, with estimates of IoT devices reaching 25 to 50 billion by 2025[15] and the average number of devices per household jumping from 10 to 50 by 2022.[16]

As consumer demand continues to grow, businesses are looking to leverage the IoT within their organizations and for big data collection.[17]

- 87% of retailers will deploy mobile point-of-sale (MPOS) devices by 2021, enabling them to scan and accept credit or debit payments anywhere in the store.
- 70% of retailers are planning investments in IoT by 2021.
- 73% of retailers consider managing big data as either "important" or "business-critical" to their operations.

Developers and companies in IoT must meet customer demand and go-to-market quickly. As a result, security measures are pushed to the back-burner.

We saw just how destructive IoT hacks could be during last year's distributed denial-of-service (DDOS) attack, which took advantage of insecure smart home devices to shut down several major websites such as Amazon, PayPal and Twitter.[18] Dyn, the domain name system (DNS) provider targeted in this instance, confirmed that the attack resulted from devices affected by the Mirai botnet, a malware that targets consumer IoT-connected devices such as webcams and printers.

In 2018, we'll see cybercriminals take this to the next level by hacking the IoT to create real-world mayhem. The interconnectedness of IoT devices make them prime targets for advanced hacks and ransomware. Imagine what people would pay if their smart thermostat or their connected vehicle were taken over?

While we've seen progress in IoT security awareness and legislation[19] and government organizations like the Federal Trade Commission[20] are taking steps to protect consumers, this incident will propel IoT developers and the government to take action to protect both organizations and consumers.

The takeaway

The number of IoT devices is rapidly increasing, making it harder to predict what commonly used product will be next to enter the connected IoT ecosystem. However, as more consumers and businesses surround themselves with smart devices, the motivation for cybercriminals only increases. Software developers need to anticipate the capabilities of today's hackers to ensure vulnerable areas are identified and addressed. Additionally, companies adopting smart devices, such as retail stores, must consider IoT-specific risks in their response plans.

2017 forecast scorecard ratings

B

1. Aftershock password breaches will expedite the death of the password.

In 2017, we saw the sale of user credentials from organizations including universities[21], large retailers[22] and governments.[23] Weak or stolen credentials continue to top the list of attack vectors, while traditional authentication continually fails to protect against cyberattacks.

A+

2. Nation-state cyberattacks will move from espionage to war.

Nation-state cyberattacks increased in number and sophistication. During the first quarter of 2017, Kaspersky Lab's Global Research and Analysis team tracked more than 100 threats targeting commercial and government organizations across 80 countries.[24] Russia, China and Iran became key players in the world of nation-state cyber espionage.

A-

3. Healthcare organizations will be the most targeted sector, with new, sophisticated attacks emerging.

From January to June 2017, 233 breach incidents were reported to the U.S. Department of Health and Human Services (HHS), the media or state attorneys general. For the 193 attacks for which there are numbers, 3,159,236 patient records were affected.[25] WannaCry, which caused significant damage, was one of the most widely known attacks.[26] Healthcare cybersecurity spending is forecasted to grow to $65 billion between 2017 and 2021.[27]

A-

4. Criminals will focus on payment-based attacks despite the EMV shift taking place over a year ago.

Although we didn't see many prominent payment-based attacks, they continued throughout 2017. Chipotle's payment processing system was breached earlier this year, prompting a conversation about the importance of companies adopting EMV chip cards.[28] On the other hand, Sears implemented the EMV system and still suffered a payment-based attack.[28]

B-

5. International data breaches will cause big headaches for multinational companies.

Fifty-one percent of the security professionals polled for the Ponemon Institute's *Data Protection Risks & Regulations in the Global Economy* reported that their companies experienced at least one global data breach in the past five years. High-level breaches like the TalkTalk[29] scam in the United Kingdom, the Wonga[30] data breach that affected the UK and Poland, and the O2 incident in Germany show international data breaches are far from over.[31]

C-

6. Virtual reality and augmented reality: new tool for hackers (other trends to watch).

While virtual reality (VR) and augmented reality (AR) were trending in many industries in 2017, they were not as prominent in the cybersecurity world. In the coming years, we may see more hackers using VR and AR capabilities to their advantage.

A

7. IRS tax scams will impact the 2016 tax season (other trends to watch).

Once again, tax season proved to be a busy time for cybercriminals. Scammers used information obtained from W2 forms to file fraudulent 2016 tax returns and receive lines of credit using Social Security numbers and more.

Previous predictions: ongoing trend or one-time fad?

Does the adage "What's old is new again" apply to cybersecurity? We went through and identified some of the major industry trends throughout the past several years to determine their staying power. The grid below includes Experian Data Breach Resolution's perspective on issues that will continue to make headlines and those that may be safe to archive.

	Ongoing trend	One-time fad
Data breach cost down — but still impactful (2014)	X	
Will the cloud and big data = big international breaches? (2014)		X
Healthcare breaches: Opening the floodgates (2014)	X	
A surge in adoption of cyber insurance (2014)	X	
Breach fatigue: Rise in consumer fraud? (2014)	X	
Beyond the regulatory checkbox (2014)	X	
Rise-and fall-of payment breaches (2015)	X	
Safeguard your Password: More hackers will target cloud data (2015)	X	
Persistent and growing threat of healthcare breaches (2015)	X	
Shifting accountability: Business leaders under increased scrutiny (2015)		X
Missing the mark: Employees will be companies' biggest threat (2015)	X	
Fresh breach surface via the Internet of Things (2015)	X	
The EMV chip and PIN liability shift will not stop payment breaches (2016)	X	
Big healthcare hacks will make the headlines but small breaches will cause the most damage (2016)	X	
Cyber conflicts between countries will leave consumers and businesses as collateral damage (2016)	X	
2016 U.S. presidential candidates and campaigns will be attractive hacking targets (2016)		X
Hacktivism will make a comeback (2016)		X
Aftershock password breaches will expedite the death of the password (2017)	X	
Nation-state cyberattacks will move from espionage to war (2017)	X	
Healthcare organizations will be the most targeted sector with new, sophisticated attacks emerging (2017)	X	
Criminals will focus on payment-based attacks despite the EMV shift taking place over a year ago (2017)	X	
International data breaches will cause big headaches for multinational companies (2017)	X	

About Experian Data Breach Resolution

Experian Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach and mitigate consumer risk following breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support and fraud resolution services while serving millions of affected consumers with proven credit and identity theft protection products. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, NetDiligence, Advisen and the Ponemon Institute RIM Council and is a founding member of the Medical Identity Fraud Alliance.

For more information, visit Experian.com/DataBreach and follow us on Twitter @Experian_DBR.

Footnotes

1. *"2 Minutes On: SWIFT — Global Banking Under Attack,"* by Roi Perez, SC Magazine UK, July 2016

2. *"40% of ICS, Critical Infrastructure Targeted by Cyberattacks,"* by Tara Seals, Infosecurity Magazine, March 2017

3. *"State Hackers 'Probably Compromised' Energy Sector says leaked GCHQ Memo,"* by Alex Hern, The Guardian, July 2017

4. *"Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure,"* The President's National Infrastructure Advisory Council, August 2017

5. *"General Data Protection Regulation,"* Council of the European Union, April 2016

6. *"Data Protection Risks & Regulations in the Global Economy,"* Experian Data Breach Resolution and Ponemon Institute

7. *"Cyberattack on parliament leaves MPs unable to access emails,"* The Guardian, June 2017

8. *"Scottish parliament hit by cyberattack similar to Westminster assault,"* by Severin Carrell, The Guardian, August 2017

9. *"DHS official: Election systems in 21 states were targeted in Russia cyberattacks,"* by Emily Tillett, CBS News, June 2017

10. *"Federal cyber assistance sought by dozens of states, local election offices during 2016 race: DHS,"* by Andrew Blake, The Washington Times, August 2017

11. *"Could AI-powered multifactor authentication kill the password at last?"* by David Braue, CSO Online, March 2017

12. *"AI Cyber Wars: Coming Soon to A Bank Near You,"* by Steve Culp, Forbes, July 2017

13. *"Internet of things: Status and implications of an increasingly connected world,"* United States Government Accountability Office, Center for Science, Technology, and Engineering, May 2017

14. *"The Internet of Things: Mapping the Value Beyond the Hype,"* McKinsey Global Institute, June 2015

15. *"OECD Digital Economy Outlook 2015,"* Organization for Economic Co-operation and Development, July 2015

16. *"Reinventing Retail: 2017 Retail Vision Study,"* Zebra Technologies, 2017

17. *"Dyn Analysis Summary of Friday October 21 Attack,"* by Scott Hilton, Dyn, October 2016

18. *"A Bipartisan Bill to Strengthen Cybersecurity for The Internet of Things,"* by Harold Stark, Forbes, August 2017

19. *"FTC Announces Internet of Things Challenge to Combat Security Vulnerabilities in Home Devices,"* Federal Trade Commission, January 2017

20. *"Cybercriminals are sharing millions of stolen university email credentials,"* by Casey Smith, USA Today, April 2017

21. *"Amazon.com's Third-Party Sellers Hit by Hackers,"* Fox Business, April 2017

22. *"Russian hackers 'traded thousands of passwords' of senior British politicians, diplomats and police,"* The Telegraph, June 2017

23. *"Destined for deletion: APTs harness wipers and file-less malware in targeted attacks,"* Kaspersky Labs, First Quarterly Summary of the APT Landscape, April 2017

24. *"Breach Barometer Report: Mid-Year Review,"* Protenus and DataBreaches.net, November 2017

25. *"WannaCrypt ransomware attack should make us wanna cry,"* by Alexander Urbelis, CNN, May 2017

26. *"Healthcare Cybersecurity Report,"* by John P. Mello, Jr., Cybersecurity Ventures, April 2017

27. *"EMV chips with that Chipotle PoS breach?"* by Robert Abel, SC Magazine, April 2017

28. *"Statement Regarding Kmart Security Incident,"* Sears Holdings, May 2017

29. *"Inside the TalkTalk 'Indian scam call centre,'"* by Geoff White, BBC News, March 2017

30. *"Wonga data breach could affect nearly 250,000 UK customers,"* by Hilary Osborne, The Guardian, April 2017

31. *"Hackers exploit SS7 telco flaw to raid German bank accounts,"* Finextra, May 2017