What CISOs Worry About in 2018

A Ponemon Institute Survey
January 9, 2018
About the survey

It’s not easy out there today being a Chief Information Security Officer. The stress and worry of data breaches — among other security concerns — are weighing on CISOs as they enter 2018.

Read more about what CISOs are thinking in the results of this survey of 612 Chief Information Security Officers and other information security professionals. The survey was fielded in November and December 2017 by Ponemon Institute, a leading research “think tank” dedicated to advancing privacy, data protection and information security practices, and was sponsored by Opus (www.opus.com), a leading global provider of compliance and risk management solutions.

The survey was created and fielded by Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute. Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management (RIM) framework. Security Magazine named him one of the “Most Influential People for Security.” In addition to institute activities, Dr. Ponemon is an adjunct professor for ethics and privacy at Carnegie Mellon University’s CIO Institute and is a fellow of the Center for Government Innovation at the Unisys Corporation.

The purpose of the survey was to understand key concerns and opinions of Chief Information Security Officers and CIOs, focused on information security and cyber-risk, as we head into 2018.

In short: What are CISOs worried about in the new year?

Key findings

- Cyber-risk and data breaches remain a key concern of Chief Information Security Officers as we enter 2018 and as today’s cyber-risk and high-profile data breaches continue. 67% of respondents believe their companies are more likely to fall victim to a cyber attack or data breach in 2018.

- Third parties are a key concern, with 60% reporting their concern of a data breach from a third party (such as a partner or vendor) has increased since last year.
• The human factor is the top security threat, with 70% of CISOs calling “lack of competent in-house staff” their number one concern and 65% stating “inadequate in-house expertise” as the top reason they are likely to have a data breach. Other key factors seen as likely reasons for a data breach include the inability to protect sensitive and confidential data from unauthorized access (59%); inability to keep up with the stealth of the attackers (56%); and failure to control third parties’ use of sensitive data (51%).

• Respondents also believe it’s highly likely they’ll experience credential theft due to a careless employee falling for a phishing scam — a 65% chance — even more likely than a malware attack, a data breach or a cyber attack.

• In the area of disruptive technologies, IoT devices are considered the most challenging to secure (60% of respondents), followed by mobile (54%) and cloud (50%).

• Not surprisingly, all this stress is taking a toll. 69% anticipate their roles will be even more stressful in 2018, while 63% expect information security budgets to decline or remain flat. 45% even fear job loss in the event of a data breach.

• On the positive side, 37% of respondents do see a path to improving their cybersecurity posture. Top improvements CISOs identified included: cybersecurity improvements (65%); improvement in staff (61%); reduction in complexity (60%); improvement in technologies (59%); and cybersecurity leadership (54%).
**Detailed findings**

**What do you predict will happen to your organization in 2018?**

*More than one response permitted*

- A careless employee fails for a phishing scam that results in credential theft: 65%
- A significant disruption to business processes caused by malware: 61%
- A cyber attack that causes significant downtime: 59%
- A data breach involving 10,000 or more customer or employee records: 53%
- Leakage of business confidential information, such as emails: 50%
- Third party misuses or shares confidential information with other third parties: 44%
- Economic espionage (theft of business-critical information): 31%
- Cyber extortion such as ransomware: 25%
- A nation state attack: 21%
- Our company will be fined for non-compliance with data protection and privacy requirements: 18%
- An attack against my company’s IT infrastructure that results in damage to property, plant, & equipment: 14%
- None of the above: 11%
- Other: 0%

While malware, cyber attacks and data breaches are clearly top of mind, human error tops the list of CISOs’ worries.
Detailed findings

What do you predict will happen to your career in 2018?

More than one response permitted

- My job will become more stressful: 69%
- I will make a lateral move within my company, but not in IT security: 44%
- I will completely change careers: 41%
- I will join another company, but not in IT security: 36%
- I will receive a promotion: 27%
- I will be terminated or demoted: 23%
- My salary will increase: 17%
- I will join another company, in IT security: 16%
- I will retire: 11%
- My job will become less stressful: 9%
- Other: 3%

CISOs are feeling the stress — even making job moves.
Detailed findings

Which of the following threats do you worry most about in 2018?

*More than one response permitted*

- The lack of competent in-house staff: 70%
- A data breach: 66%
- A cyber attack: 59%
- Inability to reduce employee negligence: 54%
- Ransomware: 48%
- Potential breach due to unsecured IoT devices in the workplace: 47%
- A third-party data breach: 42%
- Inadequate budget: 34%
- Inability to reduce malicious insider risk: 25%
- A compliance failure: 25%
- A nation state attack: 19%
- None of the above: 7%
- Other: 4%

Competence of in-house staff is the number one concern, and 66% are concerned with a data breach — but multiple concerns abound.
Detailed findings

Since last year, has your concern about experiencing a data breach caused by a business partner, vendor or contractor (third party) increased, stayed the same or decreased?

- Increase significantly: 21%
- Increase: 39%
- Stay the same: 28%
- Decrease: 10%
- Decrease significantly: 2%

Third party risk is a critical issue, with 60% saying their concern about a third party data breach has increased since last year.
Detailed findings

In 2018, do you expect your organization’s IT security budget to increase, stay the same or decrease?

- Increase significantly: 11%
- Increase: 26%
- Stay the same: 40%
- Decrease: 16%
- Decrease significantly: 7%

Despite the risks increasing, budgets are primarily flat or down.
Detailed findings

In 2018, how involved will your board of directors be in your organization’s IT security practices?

- The board of directors will become significantly more involved: 19%
- The board of directors will become more involved: 31%
- The board of directors’ involvement will stay the same: 38%
- The board of directors will become slightly less involved: 9%
- The board of directors will become significantly less involved: 3%

On the positive side, 50% say boards are becoming more involved — 19% significantly so — providing the essential backup CISOs and risk professionals require.
Detailed findings

Is your company more likely to have a data breach or cyber attack in 2018?

Yes (67%)
No (33%)

Concern levels around data breaches and cyber attacks are elevated, with 67% stating their company is more likely to have a data breach or cyber attack in 2018.
Detailed findings

If yes, why do you think you are likely to have a data breach or cyber attack in 2018?

*More than one response permitted*

- Inadequate in-house expertise: 65%
- Inability to protect sensitive & confidential data from unauthorized access: 59%
- Inability to keep up with the sophistication & stealth of the attackers: 56%
- Failure to control third parties use of our sensitive data: 51%
- Unable to replace legacy systems & technologies: 45%
- We are not providing enough training to prevent negligent behavior such as falling for a phishing scam or sharing passwords: 36%
- Inadequate budget: 33%
- Inability to control the proliferation of IoT devices in the workplace: 30%
- Lack of C-level support: 17%
- None of the above: 8%
- Other: 0%

Once again, in-house expertise is a sore point—as are the inability to protect sensitive data and to keep up as attackers become more sophisticated.
Detailed findings

What negative consequences would result if your organization had a data breach?

More than one response permitted

- Inability to recover sensitive & confidential data: 56%
- Loss of relationships with third parties & business partners: 54%
- I would lose my job: 45%
- Loss of customers: 40%
- Financial damage and fines: 36%
- Corporate reputational damage: 26%
- Revenue loss: 23%
- None of the above: 18%
- Other (please specify): 2%

The negative consequences of data breaches are often assumed to be primarily financial, but loss of data, relationships and customers are ranked most damaging.
Detailed findings

Please choose the one statement that in your opinion best describes your belief about what will happen in 2018.

- My organization’s cybersecurity posture will decline (26%)
- My organization’s cybersecurity posture will stay at about the same level (37%)
- My organization’s cybersecurity posture will improve (37%)

The outlook on cybersecurity posture isn’t as pessimistic as other results indicate — 37% do expect improvements.
Detailed findings

What success factors could drive improvement to your organization’s cybersecurity posture in 2018?

More than one response permitted

- Cyber intelligence improvements: 65%
- Improvement in staffing: 61%
- Reduction in complexity: 60%
- Improvement in technologies: 59%
- Cybersecurity leadership: 54%
- Increase in funding: 43%
- Visibility into the sensitive data accessed & used by third parties, vendors, business partners & contractors: 42%
- Ability to minimize employee-related risk: 36%
- Improvement in threat sharing: 29%
- Reduction in compliance burden: 27%
- Increase in C-level support: 16%
- None of the above: 8%
- Other: 0%

Improvements that hold promise include intelligence, people technology — and reduction in complexity. Overall, cybersecurity is complex, and CISOs need support across all fronts.
Detailed findings

In 2018, which of the following disruptive technologies will be the most challenging to secure?

*More than one response permitted*

- **IoT devices**: 60%
- **Mobile**: 54%
- **Cloud**: 50%
- **Social Media**: 38%
- **Big data analytics**: 29%
- **Artificial intelligence**: 27%
- **Blockchain (e.g., Bitcoin)**: 23%
- **Drones**: 10%
- **Robotics**: 9%

Emerging technologies also raise concerns, with the Internet of Things topping the list. As industrial and personal devices proliferate, so do unknown threats, creating potential new security challenges and a new area for CISOs to master.
Methods

What best describes your position level within the organization?

- Manager (29%)
- Director (23%)
- Executive/VP (14%)
- Supervisor (16%)
- Staff/technician (7%)
- Contractor (6%)
- Other (please specify) (5%)
Methods

What best describes your direct reporting channel?

- CIO or Head of Corporate IT (35%)
- Business Unit Leader or General Manager (23%)
- CFO, Controller, or Head of Finance (5%)
- Head of Compliance or Internal Audit (9%)
- COO or Head of Operations (10%)
- CISO/CSO or Head of IT Security (12%)
- CEO/Executive Committee (4%)
- Other (2%)
Methods

What range best describes the full-time headcount of your global organization?

- 5,001 to 10,000 (21%)
- 1,000 to 5,000 (28%)
- 10,001 to 25,000 (19%)
- 25,001 to 75,000 (8%)
- Less than 1,000 (17%)
- More than 75,000 (7%)
Methods

What best describes your organization’s primary industry classification?

- Agriculture & food services: 1%
- Communications: 2%
- Consumer products: 5%
- Defense & aerospace: 1%
- Education & research: 2%
- Energy & utilities: 5%
- Entertainment & media: 2%
- Financial services: 18%
- Health & pharmaceutical: 11%
- Hospitality: 3%
- Industrial & manufacturing: 11%
- Public sector: 10%
- Retail: 9%
- Services: 10%
- Technology & software: 8%
- Transportation: 2%
- Other: 0%
Methods

What best describes your role within your organization’s IT department?

- IT Security (35%)
- IT Management (35%)
- IT Operations (15%)
- Applications Development (6%)
- Database Administration (5%)
- IT Compliance (4%)
- I’m not involved in my organization’s IT function (0%)
Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their organization’s approach to managing data risks created through outsourcing and have involvement in managing the data risks created by outsourcing. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.
Ponemon Institute

Advancing Responsible Information Management
Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

About Opus

Free Your Business®
Opus is a leading SaaS provider of Risk and Compliance solutions. We were founded on a simple premise: that faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace.

Our mission is to free your business from the complexity and uncertainty of managing customer, supplier and third-party risks. We combine the most innovative SaaS platforms with unparalleled data solutions, helping turn information into action so your business can thrive.