Purpose and Methodology

SURVEY SAMPLE

TOTAL RESPONDENTS  
510 executives at U.S. businesses, law enforcement services and government agencies

MARGIN OF ERROR  
+/- 4.3%

AUDIENCE BASE  
CSOonline.com

SURVEY GOAL

U.S. State of Cybercrime Survey is conducted annually to gain insight and evaluate trends in the frequency and impact of cybercrime incidents, cybersecurity threats, information security spending. Additionally, the study examines the risks of third-party business partners in private and public organizations.

SURVEY METHOD

COLLECTION  
Online Questionnaire

TOTAL QUESTIONS  
61
Respondent Profile

TOTAL RESPONDENTS

510

ORIENTATION SIZE

- AVERAGE IT SECURITY BUDGET $11.0M
- AVERAGE NUMBER OF EMPLOYEES 9,795

JOB TITLE BREAKDOWN

- CORPORATE MANAGEMENT 35%
- DIRECTOR / MANAGER 23%
- EVP, SENIOR VP, VP 10%
- OTHER 30%

COMPANY SIZE

- 500+ EMPLOYEES 41%
- <500 EMPLOYEES 59%

TOP REPRESENT INDUSTRIES

- Information and Telecommunications 17%
- Banking and Finance 11%
- Electronics/Technology 11%
- Education 10%
- Services 8%
- Healthcare 5%
- Government 5%

Organizations rely on a number of information sharing organizations, but overall information sharing remains a challenge.

Q: Are you, your organization, or another individual at your organization currently a member of any of the following groups?

- United States Secret Service Electronic Crimes Task Force (ECTF) 10%
- Electronic Crimes Working Group (ECWG) 5%
- High Tech Crime Investigation Association (HTCIA) 7%
- High Tech Crime Consortium (HTCC) 4%
- US Secret Service Financial Crimes Task Force 5%
- FBI Infraguard 22%
- Department of Homeland Security (DHS) 12%
- National Cybersecurity & Communications Integration Center (NCCIC) 10%
- Information Sharing and Analysis Organizations (ISAOs) 16%
- Other government/law enforcement group 19%
The Board is Playing a Greater Role – But the Reasons Vary By Organization

Q1: How often does your CISO, CSO, or equivalent senior information security executive brief the Board of Directors on cyber risk?

Q2: How do you believe your Board of Directors views cyber risks?

Q3: Which Board Committee is responsible for cybersecurity risk management?

---

**CSOs/CISOs are reporting to the board more frequently**

- **Monthly**: 16%, 17%, 20%
- **Quarterly**: 30%, 32%, 30%
- **Annually**: 26%, 27%, 20%
- **Not at all**: 28%, 25%, 29%

---

**6 in 10 boards still only see cyber risks as an IT issue**

- As an IT issue: 63%, 61%
- As a corporate governance issue: 44%, 43%
- Other: 7%, 10%

---

**Full boards and risk committees have increasing responsibility**

- **Full Board of Directors**: 25%, 30%
- **Risk Committee**: 29%, 36%
- **Audit Committee**: 15%, 13%, 9%
- **Other**: 6%, 7%, 10%
- **None**: 29%, 26%, 15%
IT Security Budgets Continue to Increase YoY

Q: Compared with the fiscal year 2016 security budget, how did your organization’s fiscal year 2017 security budget change?

<table>
<thead>
<tr>
<th>Year</th>
<th>Increased by more than 20%</th>
<th>Increased by 10%-20%</th>
<th>Increased by less than 10%</th>
<th>Remained the same</th>
<th>Decreased by less than 10%</th>
<th>Decreased by 10%-20%</th>
<th>Decreased by more than 20%</th>
<th>Average Increase/Decrease</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>15%</td>
<td>14%</td>
<td>16%</td>
<td>48%</td>
<td></td>
<td></td>
<td></td>
<td>2% 2%</td>
</tr>
<tr>
<td>2016</td>
<td>8%</td>
<td>16%</td>
<td>21%</td>
<td>49%</td>
<td></td>
<td></td>
<td></td>
<td>1% 2%</td>
</tr>
<tr>
<td>2017</td>
<td>The average IT security budget has increased by 8% since 2016</td>
<td>10%</td>
<td>16%</td>
<td>23%</td>
<td>46%</td>
<td>1% 2%</td>
<td></td>
<td>1% 2%</td>
</tr>
</tbody>
</table>

### IT Security Investments Are Making An Impact

#### Q: To address cyber-risks, are your investments and spending focused on

- **Adding new technologies**: 40%
- **Conducting audits & assessments**: 34%
- **Adding new skills/capabilities**: 33%
- **Redesigning our cybersecurity strategy**: 25%
- **Redesigning processes**: 17%
- **Participating in knowledge sharing**: 15%
- **None of the above**: 9%

#### Q: Please estimate the total number of cybersecurity events experienced by your organization during the past 12 months

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>163.3</td>
</tr>
<tr>
<td>2016</td>
<td>161.1</td>
</tr>
<tr>
<td>2017</td>
<td>147.8</td>
</tr>
</tbody>
</table>

**Decline in Number of Security Events from 2015 to 2017**

- Decline: 8.2%
Fewer Security Events, But No Less of An Impact

Q: When compared with 2015, how did the frequency of cybersecurity events in your organization change in 2016?

- Increased
- Remained the same
- Decreased
- Don’t know/not sure

- 2015: 18%
  - Uncertainty declining, a sign of increasing network visibility
- 2016: 15%
- 2017: 12%

Q: When compared with 2015, how did monetary losses as a result of cybersecurity events in your organization change in 2016?

- 2015: 27%
  - Losses remain the same versus previous years
- 2016: 28%
- 2017: 24%
Q: Which of the following types of impacts did your organization experience in 2016 as a result of cybercrime or cybersecurity events?

1. Phishing way up over 2016

2. Ransomware growing steadily

3. Financial Fraud jumped in 2015

4. Big spike in business being the victim of Business Email Compromise

5. Sharp decline in the number of businesses that experienced no losses
Nearly One-fifth Have Experienced Critical System Disruption as A Result Of Security Events.

Q: With respect to your organization, what is the most adverse consequence that has occurred from a security event caused by an insider in the last 12 months?

- Critical system disruption to organization only: 14% (2015), 14% (2016), 14% (2017)
- Loss of confidential or proprietary information: 10% (2015), 7% (2016), 10% (2017)
- Loss of current or future revenue: 4% (2015), 4% (2016), 4% (2017)
- Harm to organization’s reputation: 6% (2015), 6% (2016), 4% (2017)
- Critical system disruption affecting customers & business partners: 6% (2015), 4% (2016), 4% (2017)
Threats Are Becoming More Difficult to Detect

Q: Which of the following types of impacts did your organization experience in 2016 as a result of cybercrime or cybersecurity events?

- Phishing: +6 pp
- Network slowdowns/downtime: +8 pp
- Application alteration: +6 pp
- Card-not-present fraud: +7 pp

Q: On average, how much time passed between the date you believe an intrusion began and the date it was discovered?

- 2015: 57.6 Days
- 2016: 80.6 Days
- 2017: 92.2 Days

Average time to intrusion discovery has grown by more than one month since 2015.

pp = percentage points
Despite Confidence in Internal Expertise, Concern Level Rises

Q: Are you more concerned or less concerned about cybersecurity threats to your organization in 2017 than you were in 2016?

- Level of concern has not changed
- Less concerned
- More concerned

<table>
<thead>
<tr>
<th>Year</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>64%</td>
<td>74%</td>
<td></td>
</tr>
</tbody>
</table>

Big jump in concern about security threats

Q: As new technologies or processes are introduced into your organization (cloud, mobile, social, data analytics, mobile payment systems, connected devices/IoT, etc.), does your organization have the expertise to address the cyber-risks associated with them?

- 76% Yes
- 8% Don't know
- 16% No

Business feel as though they have the expertise to address the risks associated with new technologies

Q: Please indicate which of the following resulted from the cybersecurity incidents your organization experienced in 2016.

Top Impacts:

15% Notification of Individuals: We had to notify the impacted individuals of the breach
10% We suffered Financial losses
8% Notification of Business Partners: We had to notify the impacted businesses
8% Notification of Regulators: We had to notify regulatory bodies
7% Notification of Law Enforcement: We had to notify government entities (USSS, FBI, etc.)
6% IP, trade secrets or other proprietary information was stolen
6% Our organization's brand or reputation was damaged
Outsiders Are Generally Perceived as the Bigger Threat

Q: Which of the following groups posed the greatest cyber threat to your organization during the past 12 months?

- 4% | Organized crime
- 5% | Foreign entities & org.
- 8% | Foreign Nation-States
- 16% | Current employees
- 26% | Hackers (those that do not fall into any of the other choices listed above)

Q: In general, cybercrimes were more costly or damaging to your organization when caused by:

- 31% | Don’t know/not sure
- 39% | Outsiders: Someone who has never had authorized access to an organization's systems or networks
- 29% | Insiders: Current or former employee, service provider, or contractor
- 5% | Foreign entities & org.
- 5% | Foreign Nation-States
- 6% | Organized crime
- 13% | Current employees
- 33% | Hackers (those that do not fall into any of the other choices listed above)
Sources of Security Incidents

Q: Please indicate the source(s) of these security incidents, to the best of your knowledge.

- Virus, worms or other malicious code
- Phishing
- Ransomware
- Unauthorized access
- Spyware
- Sabotage of systems
- Business email compromise
- OSs/files altered
- Denial of service attacks
- Systems destroyed
- Financial fraud
- Illegal generation of spam email
- Customer records compromised
- Website defaced
- Systems used as part of botnets
- Unauthorized system storage
- Sensitive information exposed
- Card-not-present fraud
- Email/applications unavailable
- Theft of PII
- Software applications altered
- Identity theft
- Employee records compromised
- Unauthorized outgoing spam
- Confidential records compromised
- Loss of internal records
- Payment card systems compromised
- Point-of-sale systems compromised
- Network slowed/unavailable
- Extortion
- Theft of medical information
- Mobile payment system...

Most Insider Security Events Are Caused By Employee Negligence, Highlighting The Need For Better Education Programs

Q: Of the security incidents you know you experienced and for which you were able to attribute to an insider, what do you believe were the motivations behind the attacks?

- Unintentional/accidental: 28%
- Intentional attacks: 18%
- "Insider" credentials stolen: 8%
- Don't know: 11%

Note: 45% report not applicable

Q: In your organization, which of these users pose the greatest risk for an Insider Threat incident?

- Innocent employee who falls for a phishing or hacker scam, or whose credentials were otherwise comprised: 47%
- Careless employee who consistently blends work and personal usage: 23%
- Don't know: 14%
- The disgruntled employee: 8%

Note: 45% report not applicable
Crime & Punishment: Increase in Targeted Attacks

Q: If any cybersecurity events or cybercrimes were not referred for legal action, please indicate the reason(s) they were not referred.

- 44% Could not identify the individual/individuals responsible for committing the cybercrime
- 40% Damage level insufficient to warrant prosecution
- 32% Lack of evidence not enough information to prosecute
- 7% Concerns about liability
- 7% Concerns about liability

Q: Please estimate the total monetary value of losses your organization sustained due to cybercrime and advanced persistent threats during the past 12 months, including those costs associated with resolving all issues associated with the incident.

Percentage of people answered “Don’t know”

- 58% in 2016
- 65% in 2017

Increasingly, businesses struggle to understand how much a security incident costs

Q: When considering the financial losses or costs to your company from those targeted attacks aimed at your company, has the financial loss or cost increased or decreased versus the previous year?

Percentage of people answered “Don’t know”

- 40% in 2016
- 31% in 2017

Q: Of the security events your company experienced during the past 12 months, what percentage of these events were:

- Targeted attacks aimed at your company, your employees, your resources, or your customers
  - 2015: 28%
  - 2016: 32%
  - 2017: 39%
- Non-specific or incidental attacks/malware that happened to impact your company, employees, resources, or customers
  - 2015: 72%
  - 2016: 68%
  - 2017: 61%

Q: Of the security events your company experienced during the past 12 months that caused financial loss or cost, what percentage of these events were:

- Targeted attacks aimed at your company, your employees, your resources, or your customers
  - 2015: 28%
  - 2016: 33%
  - 2017: 44%
- Non-specific or incidental attacks/malware that happened to impact your company, employees, resources, or customers
  - 2015: 72%
  - 2016: 67%
  - 2017: 56%

Defending the Digital Business Ecosystem – Are Businesses Doing Enough?

Q: Do you have a process for evaluating the cybersecurity of supply chain/business ecosystem partners with whom you share data or network access (joint ventures, strategic partnerships, upstream or downstream supply chain, etc.)?

- 16% | Don’t know
- 35% | No, we don’t have a process
- 11% | Yes, but only after we are already conducting business with them
- 38% | Yes, we do so prior to conducting business with them

Q: On average, how often do you evaluate the security of supply chain/business ecosystem partners with which you share data or network access?

- 22% | Don’t know/not sure
- 30% | We don’t typically evaluate third parties
- 17% | More than once per year
- 30% | Once per year or less

Q: Has due diligence of supply chain/business ecosystem partners resulted in termination of a contract or business relationship?

- 28% | Don’t know/not sure
- 51% | No
- 17% | More than once per year
- 30% | Once per year or less

Q: Do you conduct incident response planning/conduct table top exercises with your supply chain/business ecosystem partners?

- 20% | Don’t know/not sure
- 56% | No, we do not include third parties in our incident response planning
- 5% | Yes, but only after an incident occurs
- 5% | Yes, once every two years

Q: Do you have Service-Level Agreement with your supply chain/business ecosystem partners that specifies minimum cybersecurity standards?

- 35% | No
- 22% | Don’t know/not sure
- 51% | No, we do not include third parties in our incident response planning
- 5% | Yes, once every two years
- 14% | Yes, once per year or less
- 43% | Yes
Though Half of All Organizations Monitor User Behavior, Just One-third Have A Way To Interpret Intent

Q: Does your organization currently:

- Have a way to understand employee behavior and intent as they interact with your IP and other business data? 33% Yes, 48% No, 19% Don’t know
- Monitor user behavior 58% Yes, 31% No, 10% Don’t know
- Have visibility into data protection vulnerabilities from use of non-IT supported cloud applications 50% Yes, 26% No, 23% Don’t know

Just One-third Are Measuring the Effectiveness of Security Programs Annually or More Often

Q: Do you have a methodology that helps you determine the effectiveness of your organization's security programs based on clear measures?

- Yes: 53%
  - Yes, more than once per year: 24%
  - Yes, once a year: 15%
  - Yes, but less than once per year: 13%
- No: 30%
- Don't know/not sure: 17%
In Most Cases, Cybercrimes Committed By Insiders Are Handled Internally


Q: Please indicate the percentage of cybercrimes committed by insiders were:

- Handled internally without involving legal action or law: 76%
- Handled internally with legal action: 13%
- Handled externally by notifying law enforcement: 7%
- Handled externally by filing a civil action: 5%
Q: Describe your organization’s current approach to insider threat funding.

- **22%** IT initiative to upgrade security controls
- **18%** IT budget is flexible if a solution is clearly superior and/or cost-cutting
- **12%** Ongoing top-down company commitment and ample budget to stay ahead of the threats
- **7%** Legal and compliance initiative to eliminate non-compliance fines or audit risks
- **3%** HR organization initiative to observe user activity to protect both the employee and organization
- **19%** Don’t know
- **20%** Not applicable
Technology Usage and Effectiveness

Q: How effective do you consider each of the following technologies in place at your organization in detecting and/or countering security events?

### Average Effectiveness – Top Ranked Technologies

(1=Not at all effective; 5=Extremely effective)

<table>
<thead>
<tr>
<th>Technology</th>
<th>Average Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor/strong authentication</td>
<td>3.5</td>
</tr>
<tr>
<td>Encryption</td>
<td>3.44</td>
</tr>
<tr>
<td>Firewalls</td>
<td></td>
</tr>
<tr>
<td>Role-based authentication</td>
<td>3.28</td>
</tr>
<tr>
<td>Biometrics</td>
<td>3.27</td>
</tr>
<tr>
<td>Access controls</td>
<td>3.26</td>
</tr>
<tr>
<td>Host-based firewalls</td>
<td>3.26</td>
</tr>
<tr>
<td>Network Access Control (NAC)</td>
<td>3.26</td>
</tr>
<tr>
<td>Wireless encryption/protection</td>
<td>3.25</td>
</tr>
<tr>
<td>Identity management system</td>
<td>3.22</td>
</tr>
<tr>
<td>Electronic access control systems</td>
<td>3.21</td>
</tr>
<tr>
<td>Policy-based network connections &amp; enforcement</td>
<td>3.21</td>
</tr>
<tr>
<td>Automated patch management</td>
<td>3.21</td>
</tr>
<tr>
<td>Network IDS/IPS</td>
<td>3.2</td>
</tr>
<tr>
<td>Network-based anti-virus</td>
<td>3.19</td>
</tr>
</tbody>
</table>

### Percent with Each Technology in Use

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percent with Each Technology in Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-factor/strong authentication</td>
<td>73%</td>
</tr>
<tr>
<td>Encryption</td>
<td>78%</td>
</tr>
<tr>
<td>Firewalls</td>
<td>92%</td>
</tr>
<tr>
<td>Role-based authentication</td>
<td>67%</td>
</tr>
<tr>
<td>Biometrics</td>
<td>83%</td>
</tr>
<tr>
<td>Access controls</td>
<td>72%</td>
</tr>
<tr>
<td>Host-based firewalls</td>
<td>80%</td>
</tr>
<tr>
<td>Network Access Control (NAC)</td>
<td>70%</td>
</tr>
<tr>
<td>Wireless encryption/protection</td>
<td>80%</td>
</tr>
<tr>
<td>Identity management system</td>
<td>63%</td>
</tr>
<tr>
<td>Electronic access control systems</td>
<td>75%</td>
</tr>
<tr>
<td>Policy-based network connections &amp; enforcement</td>
<td>75%</td>
</tr>
<tr>
<td>Automated patch management</td>
<td>75%</td>
</tr>
<tr>
<td>Network IDS/IPS</td>
<td>72%</td>
</tr>
<tr>
<td>Network-based anti-virus</td>
<td>87%</td>
</tr>
</tbody>
</table>
So what do businesses tell us works?

Q: Have any of the following security policies and procedures at your organization supported or played a role in the following:

Base: Organization uses security policies and procedures in an attempt to prevent or reduce security events (not 'None of the above', 'Not applicable/no written policy in place', or 'Don't know')

- **Deterrence of a potential criminal**
  - Physical security: 57%
  - Encryption: 53%
  - Patch management: 53%
  - Strong password controls: 51%
  - Multi-factor authentication: 50%

- **Detection of a criminal**
  - Logging and monitoring: 46%
  - Application security: 26%
  - Appropriate use technology: 25%
  - Behavior monitoring: 25%
  - Incident response: 24%

- **Termination of an employee or contractor**
  - Appropriate use of technology policies: 41%
  - Logging and monitoring: 38%
  - Behavior monitoring: 26%
  - Authorization: based on roles: 22%
  - Compliance w/ legal req: 21%

- **Prosecution of an alleged criminal**
  - Logging and monitoring: 37%
  - Application security: 24%
  - Incident response: 21%
  - Appropriate use of technology: 20%
  - Compliance w/ legal req: 19%

26% Are Using Dedicated Mobile Security Technologies to Secure Devices

Q: Which of the following does your company utilize to secure mobile devices (e.g., smartphones, tablets)?

- Remote wipe capability: 26%
- Mobile device management software: 39%
- Device encryption: 35%
- Strong authentication on devices: 34%
- Mobile security technologies: 32%
Companies Monitor A Variety Of Sources to Keep Current on Threats, though Less Than One-third Update Cyber Response Plans Frequently

Q: Does your organization have a formalized plan outlining policies and procedures for reporting and responding to cyber events committed against your organization?

- Yes, and we test it at least once per year: 52%
- No plans at this time or in the near future: 35%
- No plan currently, but intend to have one within the next 12 months: 19%
- Yes, but we do not test it at least once per year: 23%
- Don't know/not sure: 16%
- None: 6%

Q: Please identify all sources you monitor to keep up with current trends, threats, vulnerabilities, technology, and warnings.

- Cybersecurity websites and emails: 75%
- Subscription-based services (free): 68%
- Peers: 54%
- Print publications or websites: 47%
- Industrial trade associations: 40%
- Subscription-based services (paid): 39%
- Government websites & emails (other than DHS): 38%
- Information Sharing & Analysis Centers (ISACs): 33%
- Department of Homeland Security (DHS): 33%
- Information Sharing & Analysis Organizations (ISAOs): 19%
- Other: 5%
- None: 6%

Conclusions

- Organizations rely on a number of information sharing organizations, but overall sharing remains a challenge.
- The board of directors is playing a greater role – but the reasons vary by organization.
- While IT security budgets continue to grow, and those investments are driving down the number of known security events, monetary losses haven’t really moved.
- Successful phishing and ransomware attacks are climbing – and threats, overall, are becoming more difficult to detect.
- Concerns about security threats took a significant jump this year.
- Outsiders continue to be perceived as the greater threat and targeted attacks are becoming more prevalent. At the same time, Insiders are falling for phishing scams and being careless, pointing to the need for better security & awareness training.
- There remain significant holes in our digital business ecosystems.
- While businesses collect lots of data, they struggle to identify intent in it – and only slightly more than half measure the effectiveness of their efforts.
- Businesses still, overwhelmingly, handle the dirty laundry of insider attacks themselves without involving law enforcement.
- Logging & Monitoring, as well as Encryption, continue to be perceived as highly effective in addressing cybercrime concerns.