tsi

# TSI’s Information Security Overview

2016

# The Current Information Security Landscape

- Info Sec is a permanent cost that organizations need to be prepared to deal with and incorporate in their data protection strategies.
- The biggest financial consequence to organizations that experience a data breach is lost business.
- Organizations are recognizing that the longer it takes to detect and contain a data breach the more costly it becomes to resolve.
- The more customer turnover, the higher the per capita cost of the data breach.
- Detection and escalation costs are at a record high. Average detection and escalation costs increased dramatically from $0.61 million to $0.73 million, suggesting that companies are investing more heavily in these activities.
- Heavily regulated industries such as healthcare, life science and financial services, tend to have a per capita data breach cost substantially above the overall mean of $221. In contrast, public sector (government), hospitality and research had a per capita cost well below the overall mean value.
  - Healthcare: $402 per record
  - Financial Institutions: $264 per record
  - Education: $220 per record
  - Commercial & SME: $218 per record
  - Government: $86 per record
- Malicious or criminal attacks continued to be the primary cause of data breach and were the most costly. 50% of incidents involved a malicious or criminal attack, 23% of incidents were caused by negligent employees, and 27% involved system glitches that included both IT and business process failures.
- Certain factors decreased the cost of data breach. Incident response plans and teams in place, extensive use of encryption, employee training, BCM involvement or extensive use of DLP reduced the cost of data breach. Data breaches due to third party error, extensive cloud migration or a rush to notify increased the cost.

  a. *Sources:*

     i. *"Cost of Data Breach Study: Global Analysis" | IBM/ Ponemon*

     ii. *"ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC*

     iii. *"2015 Global Cybersecurity Status Report" | ISACA International*

# The Facts & Figures

**2015 Data Breach Category Summary**

| BU | # of breaches | % total breaches | # of records | % total records |
|---|---|---|---|---|
| **Finance** | 71 | 9.1% | 5,063,044 | 2.8% |
| **Commercial & SME** | 312 | 40% | 16,191,017 | 9.1% |
| **Education** | 58 | 7.4% | 759,600 | 0.4% |
| **Government** | 63 | 8.1% | 34,222,763 | 19.2% |
| **Healthcare** | 276 | 35.4% | 121,629,812 | 68.4% |

- 2015 Totals: 780 reported breaches; 177,866,236 records
  - *Source: "ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC*

-----

- $7.01 million is the average total cost of a data breach. The average cost per each lost or stolen record containing confidential and sensitive data was $221. The industry with the highest cost per stolen record was healthcare, at $402 per record.
  - *Source: "Cost of Data Breach Study: Global Analysis" | IBM / Ponemon*
- In 2015, there were 38% more information security incidents detected than in 2014.
  - *Source: "The Global State of Information Security Survey 2016" | PWC*
- At least 52% of CISOs felt that a successful cyberattack against their network would take place within the year.
  - *Source: "2015 Cyberthreat Defense Report" | CyberEdge Group*
- 74% of CISOs are concerned about employees stealing sensitive company information.
  - *Source: "SANS 2015 Survey on Insider Threats" | SpectorSoft*
- Only 38% of global organizations claim they are prepared to handle a sophisticated cyberattack.
  - *Source: "2015 Global Cybersecurity Status Report" | ISACA International*

# How TSI Addresses Info Sec

The most profitable investments companies can make in order to mitigate the risk of future breaches are incident response plans, extensive use of encryption, participation in threat sharing, employee training, business continuity management, and data loss prevention technologies. TSI has invested heavily in all six and each is a key component of our Information Security Management System (ISMS).

## "TSI's ISMS reduces risk and minimizes direct, indirect, and opportunity costs associated with a breach."

- Indirect costs: What the company spends on existing internal resources to deal with a data breach. These costs could include the time employees spend on data breach notification efforts or investigations of the incident. Indirect costs also include the loss of brand value, reputation, and customer churn.
- Direct costs: What companies spend to minimize the consequences of a data breach and to assist victims. These costs include engaging forensic experts to help investigate the data breach, hiring a law firm, and offering victims identity protection services.
- Opportunity costs: The cost resulting from lost business opportunities as a consequence of negative reputation effects after the breach has been reported to victims and publicly revealed to the media (both turnover of existing customers and diminished customer acquisition).

## "TSI is a certified FISMA, PCI DSS 3.1, and SSAE 16 (SOC 1) compliant service provider. Are you? Are your vendors?"

As a result of the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) maintains a catalog of security controls for all US federal information system called "NIST Special Publication 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations." TSI utilizes these proven, government-approved security controls and encryption technologies in all IT systems that process, store, and transmit confidential data to preclude disclosure to unauthorized internal and external parties.

## "TSI have made extensive investments in both talent and cutting-edge technology to ensure our IT systems and data remain secure."

Shawn Greenwald, CTO, and Toby Miller, Director of IT Security, and Torrey Gasch, Director of Business Continuity, all understand the absolute necessity of maintaining an ISMS of the highest quality. That's why we've invested in a SUPERNAP colocation data center – the same data center utilized by the likes of Google, Intel, Deloitte, and JP Morgan Chase – as well as a full suite of data loss prevention (DLP) software from Trend Micro.