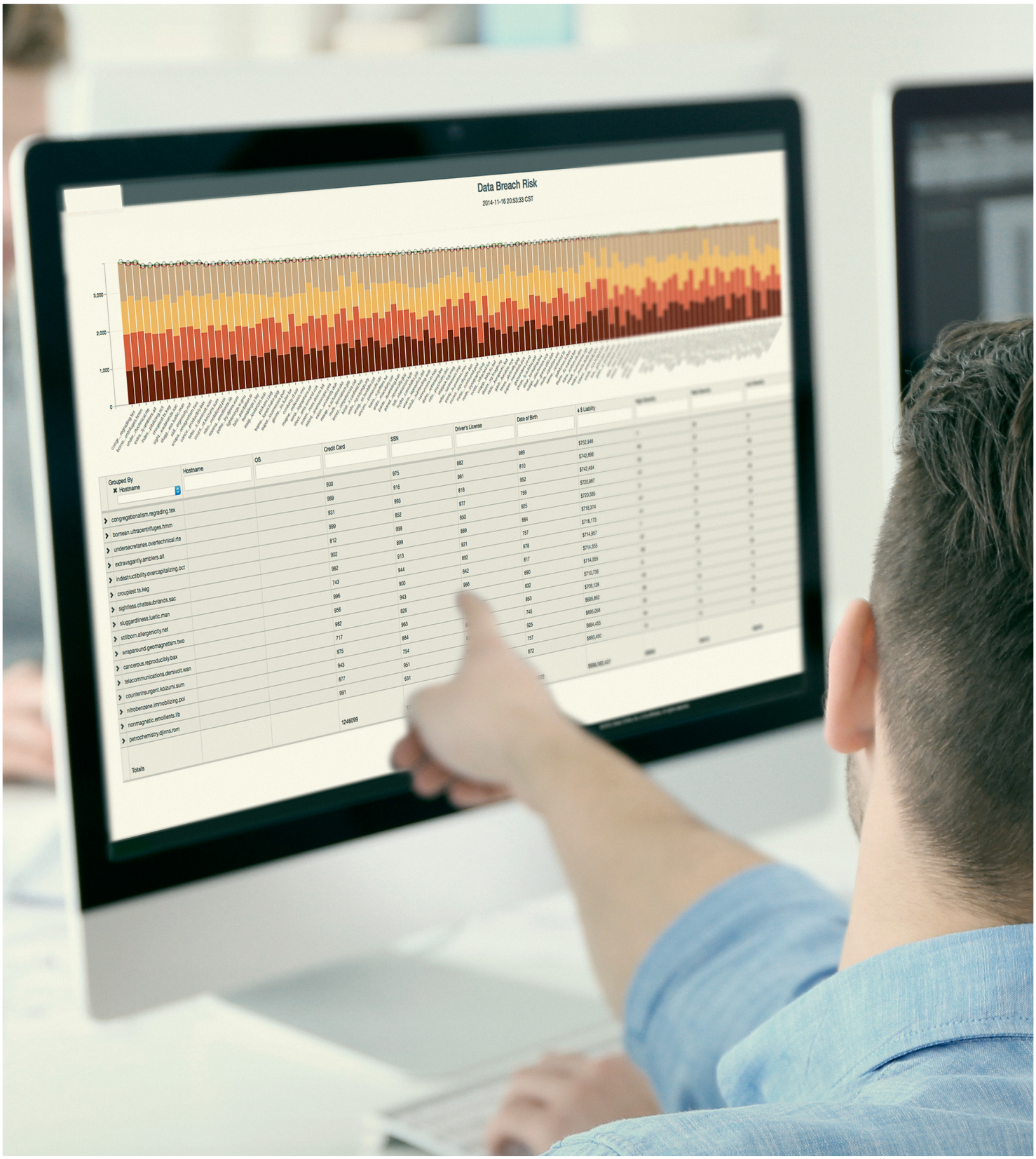


MSP RISK INTELLIGENCE

DATA BREACH RISK BRIEF

solarwinds msp

Banking on traditional backup and recovery methods to protect your customers' data could leave you and your customer with an unexpected surprise.

INTRODUCTION

Data Breach Risk Brief

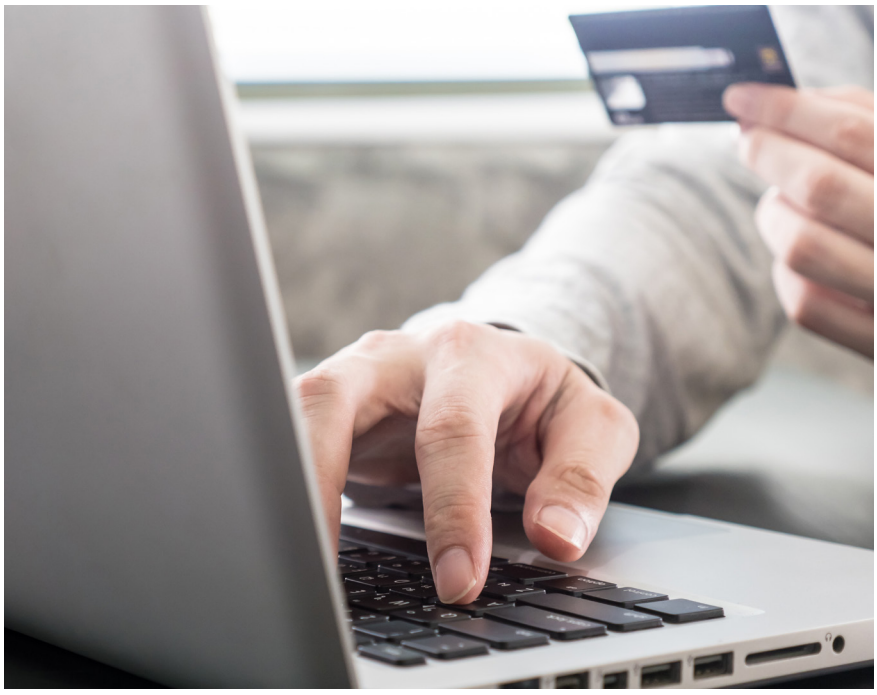
Boards are demanding oversight of their organization's risk posture from the Chief Information Security Officer (CISO). But much data has moved beyond the visibility and control of the security team, and into the hands of employees. We believe that CISOs will be most effective when they engage directly with the business, connecting risk to business outcomes.

Real Data from Customers

SolarWinds® MSP Risk Intelligence provides a risk intelligence platform that prioritizes risk in the language of the C-suite—dollars. We have collected data on unprotected data, vulnerabilities, and access permissions from over 700,000 customer devices using our technology. Our customers range from small to large organizations and represent diverse industries from higher education to financial institutions to retail. The results of our findings are outlined in the rest of this brief.

The data collected answers:

- What sensitive data do organizations typically have and who has access?
- How can attackers get to it?
- What will it cost when breached?



87% of all desktops show credit card data being stored.

OUR GOAL IS TO CREATE URGENCY

This brief shares some of the key data points collected from the 700,000 devices. Our goal in sharing this data is to escalate the urgency for CISOs to improve communication with their businesses.

In almost every case, the security leaders we worked with were surprised by where unprotected data resides and the liability cost if breached. The results clearly prioritized which devices should be remediated first to reduce total risk exposure for the organizations.

Tape backups are often performed manually, which means that missed backups and other human errors are inevitable.

DATA BREACH RISK BRIEF

Key Findings

Collected from over 700,000 data points:

- Highest data breach risk (liability) detected: $400 million on a single server
- Average liability of a server: $301,098
- Average liability of a desktop: $48,843

Breakdown of liability:

- 5% of desktops/laptops have $25,000 of liability or less
- 92% of desktops/laptops have between $25,000–$250,000 of liability
- 3% of desktops/laptops have $250,000 or more in liability
- 87% of all desktops show credit card data being stored
- 36% also show social security numbers

The most common vulnerabilities resided in:

- OS
- Third-party browsers
- Applications such as Adobe Flash, Adobe AIR, and Java

Applying the Results

What should a company of 250 employees take from this report? If three percent of desktops and laptops have over $250,000 in data breach risk, then a company of 250 employees would:

- Have just seven computers that, if breached, would likely cost the company over $2 million.
- Immediately deploy the security team to remediate those seven computers.
- Provide security awareness training for the computer owners.
- Then present to the board in a clear dollar amount how the total risk exposure of the organization was just reduced by over $2 million.

MSP Risk Intelligence liability data is a proprietary calculation of the cost of a breach weighted by real-time sensitive data, vulnerabilities, and access permissions on a device.

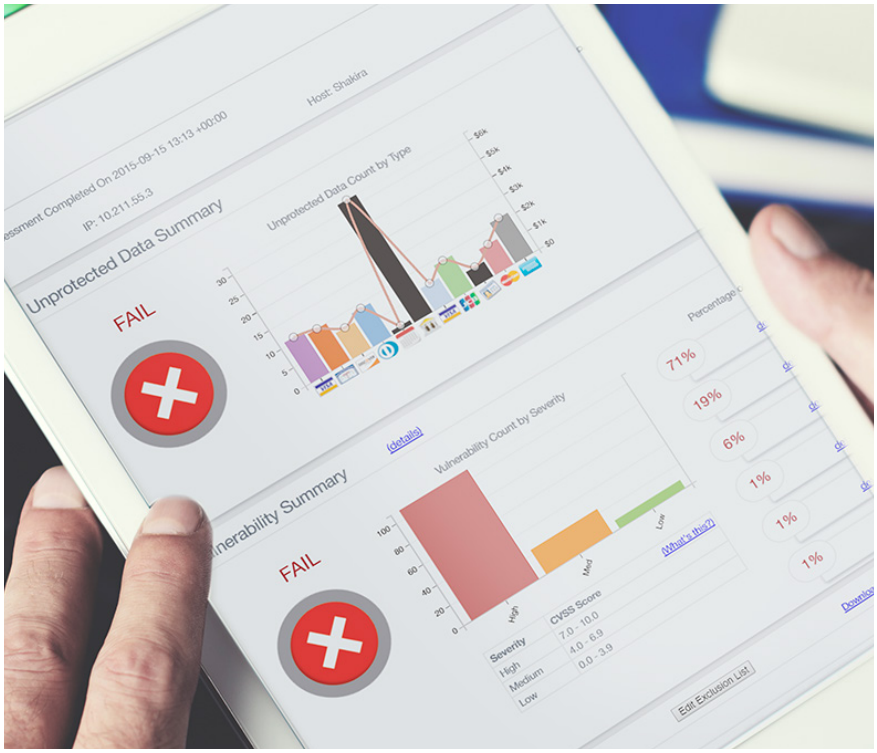
DATA BREACH RISK BRIEF

Methodology

This study includes 700,000 scans of devices that were used by customers of diverse sizes and industries.

Devices included servers, desktops, and laptops. MSP Risk Intelligence also scans mobile devices like smartphones and tablets, but that data is not included in this report.

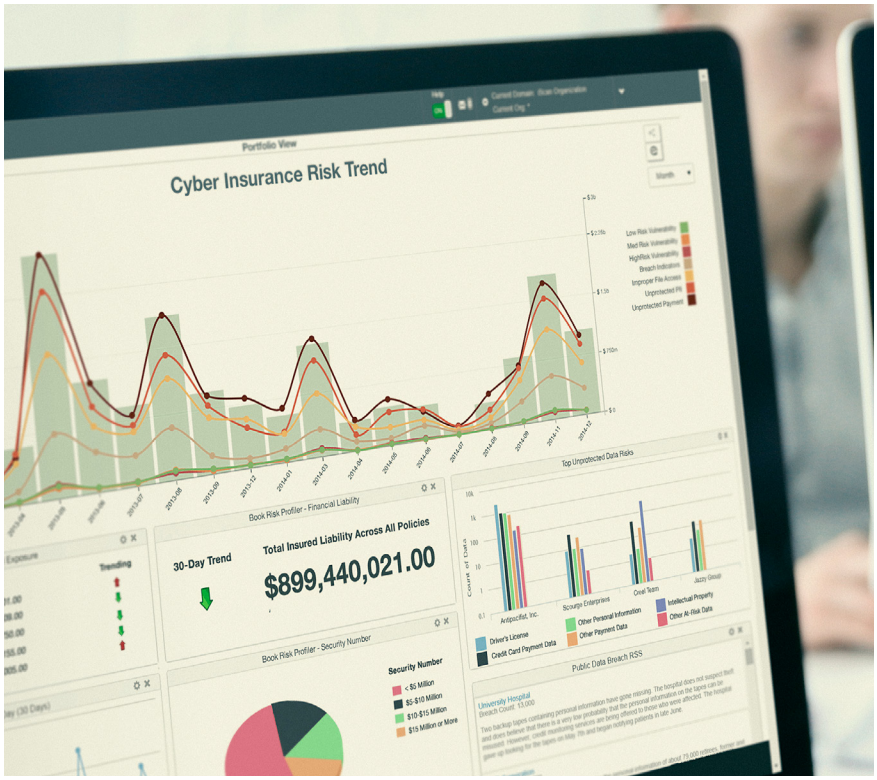
- Data was collected over a two-year period.
- MSP Risk Intelligence currently supports scanning for intellectual property and ACH data. This data is not included in the results.
- MSP Risk Intelligence liability data is a proprietary calculation of the cost of a breach weighted by real-time sensitive data, vulnerabilities, and access permissions on a device. Breach cost data considers data from sources such as Ponemon Institute and Verizon, but weights cost with the actual risk of each device.



ABOUT MSP RISK INTELLIGENCE

MSP Risk Intelligence is the industry's first data breach risk intelligence platform that puts a real-time dollar number on an organization's security risk. MSP Risk Intelligence's patented discovery process uncovers sensitive data, vulnerabilities and access permissions, and then financially prioritizes the results in reports that speak the language of the board—dollars. Now CISOs can make informed resource decisions and educate board members on the impact of security initiatives.

To find out more information about the MSP Risk Intelligence platform and to get an immediate free trial, visit the SolarWinds MSP website.



LAYERED SECURITY

COLLECTIVE INTELLIGENCE

CROSS-PLATFORM

SolarWinds MSP empowers MSPs of every size and scale worldwide to create highly efficient and profitable businesses that drive a measurable competitive advantage. Integrated solutions including automation, security, and network and service management—both on-premises and in the cloud, backed by actionable data insights, help MSPs get the job done easier and faster. SolarWinds MSP helps MSPs focus on what matters most—meeting their SLAs and creating a profitable business.

For more information, visit **www.solarwindsmsp.com**

RIPF00124EN1116

WWW.SOLARWINDSMSP.COM

solarwinds msp