Whitepaper

cipher

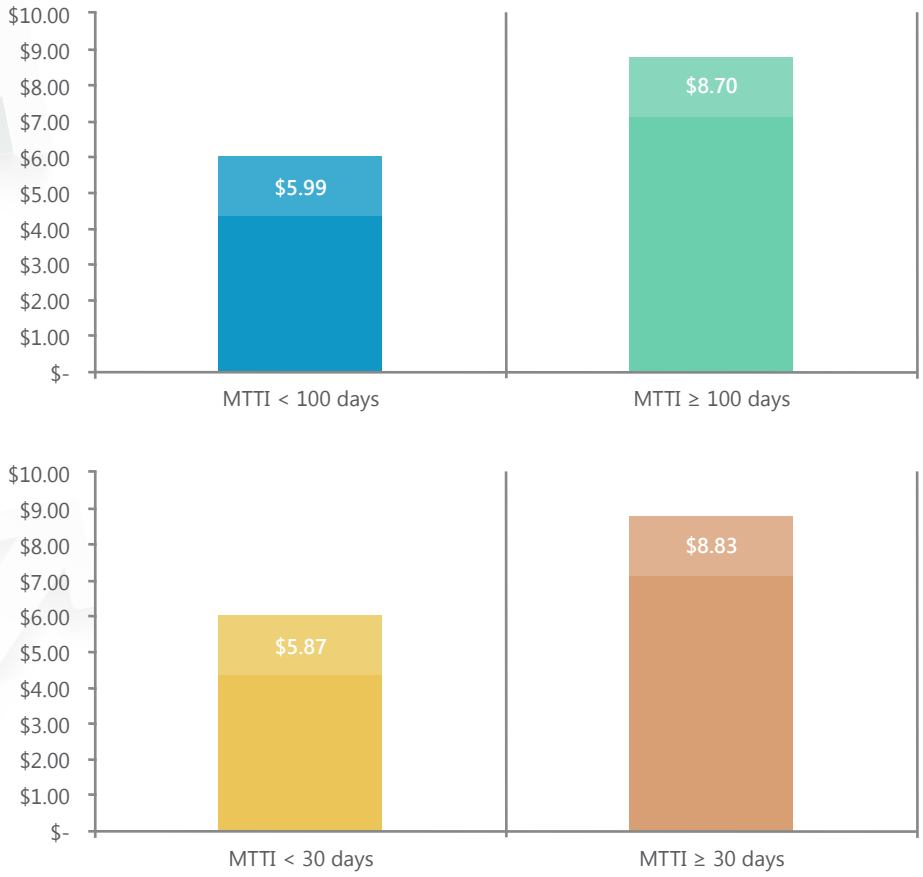
we secure your business

# THE RETURN ON INVESTMENT OF A BALANCED CYBER SECURITY STRATEGY

# WHY A BALANCED, PROACTIVE APPROACH IS BETTER – MOST HAVE PREVENTION BIAS

Small to Medium Businesses **(SMB)** have many of the same security interests and concerns as large enterprises, but typically lack the breadth and depth of resources of their larger counterparts. What defines the SMB classification? According to Gartner:

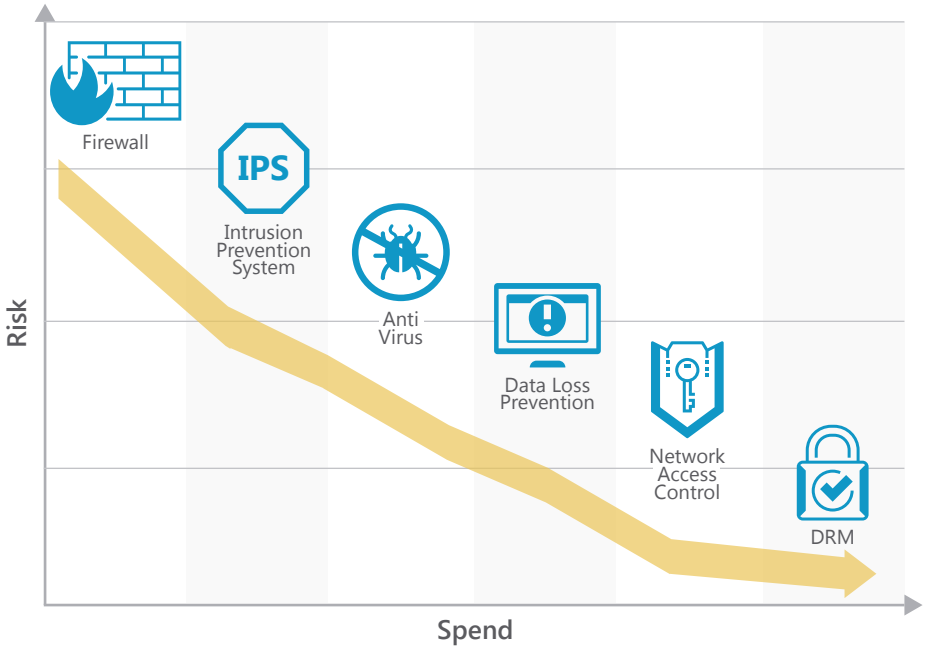
Statistics from the Ponemon Institute's 2017 report on breach costs shows that not only do we have a prevention bias, it also costs us money. The Mean Time To Identify **(MTTI)** breaches among U.S. companies in 2016 was 206 days, up from 191 days in 2016. The Mean Time To Contain **(MTTC)** was an additional 55 days, down from 2016's 58.




*Dollar figures listed in millions*

Even though most will freely admit that we cannot prevent a breach – if a threat actor or group wants to break in and is persistent enough for a long enough period, they will likely succeed – companies in the U.S. show an inherent bias toward spending on prevention.

**Firewalls, IPS, Anti-Virus, DLP, NAC, DRM, Endpoint Agents** -- despite a pervasive awareness that at some point the effectiveness of preventative spend declines, we have an inclination toward investing in yet more and more prevention.




An appropriate balance between **Prevention**, **Detection**, and **Response** is needed. Some examples of detection – consisting of monitoring and alerting --include log aggregation and the use of a SIEM; ensuring 24/7 coverage through automation, staffing, or the use of an MSSP; and tuning your policies over time so that only actionable events result in an alert.

Examples of response activities include having a dedicated Incident Response Team or available MSS Red Team; having a documented playbook or collection of procedures to follow should a breach be identified; tracking metrics to gain insight into trends in your environment; and vulnerability and penetration testing, which can be conducted internally or using a third party to guarantee unbiased results.

Overall, a proactive and balanced approach to security operation across all three stages decreases your likelihood of breaches and prepares your organization to handle them when a security incident does occur.

# BECKSTROM'S LAW & RETURN ON SECURITY INVESTMENT (ROSI)

Beckstrom's Law is a method of computing ROI by showing the value of a security initiative. Rod Beckstrom is an author, high-tech entrepreneur, former CEO and President of ICANN, and previously served as Director of the National Cybersecurity Center within the Department of Homeland Security. Beckstrom's Law, in its simplest form, states the value of a network as the benefit value of all transactions minus the cost of all transactions.

**Value = Benefit – Cost**

A simple example would be if it costs a person $25 to buy a book in a store, and $15 to buy it online, the value of the network to that person is $10. If that applies to 1000 people, the network's value is $10,000. If there are ten similar scenarios every work day, $100,000. Knowing that there are 365 days a year, with an average 261 of them being work days, the network is potentially worth $26.1 million over the course of a year on this basis alone.

A minor addition to Beckstrom's Law reveals Beckstrom's Law, Security Model: the value of a security initiative is equal to the benefit value of all transactions minus the cost of the security investments minus the amount of residual loss (in the form of lost productivity and corresponding manpower costs, lost revenue, labor cost to remediate, etc.).

**V = B – SI – L**

For example, if a car is worth $25,000, and a security alarm system costs $2500; and a thief attempts to break in, aborting his attempt due to triggering the alarm after causing $500 in damage to the car's locks; the value of the security system is $22,000.

**V = B – SI – L**
**V = $25,000 - $2500 - $500**
**V = $22,000**

You could apply this reasoning to the case of anti-virus systems. For example, a global company is getting a high volume of viruses, as many as 1000 per month. Virus occurrences that resulted in an offline scan or re-image take an average of 3 hours to remediate. Considering that the average salary for an employee at the company is $75 per hour including all benefits and that both a help desk tech and the infected employee were involved, such incidents cost $450 each. Over the course of a year, 4500 such virus incidents occurred, representing over $2 million of labor costs in the form of productivity lost. If virus incidence could be reduced by 25%, it would be worth $500,000. Residual losses such as missed deadlines and incomplete tasking are estimated at $5,000 monthly.

Applying everything to Beckstrom's Law, expecting to reduce virus incidents by 25% and deploying a $75,000 endpoint agent, yields the following, including adjusted residual loss:

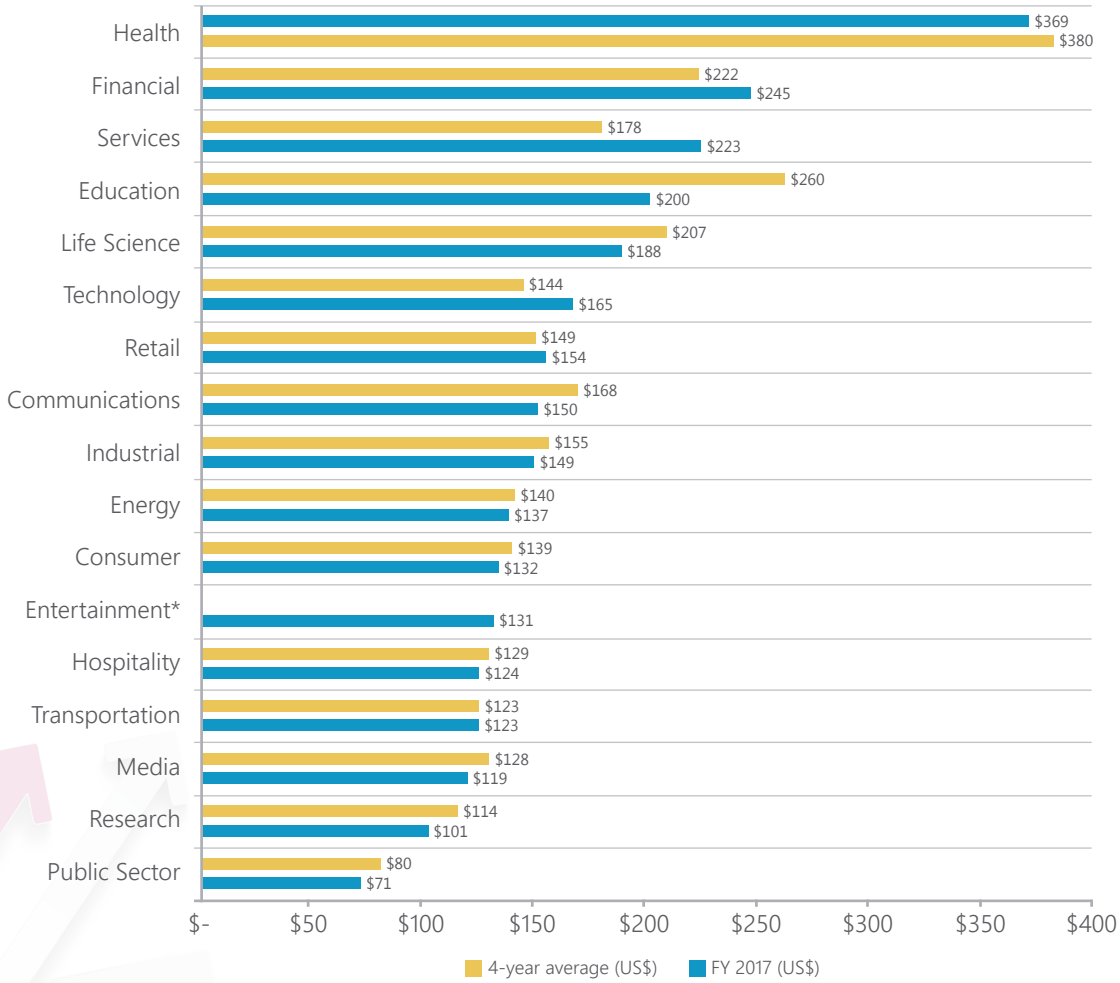
**V = B – SI – L**
**V = $500,000 - $75,000 - $45,000**
**V = $385,000**

That's a decent ROI. What if you could see a 75% reduction in virus incidents?

**V = B – SI – L**
**V = $1,500,000 - $75,000 - $15,000**
**V = $1,395,000**

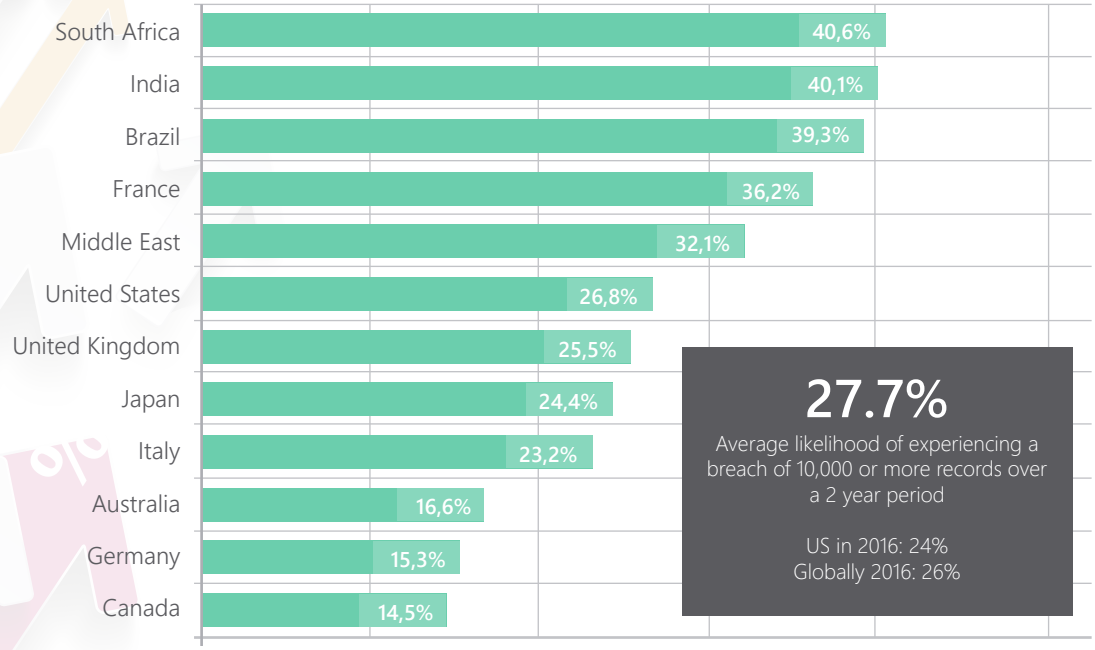
## THE REAL COST OF DATA BREACHES

With the Ponemon Institute's Report on Breach Costs, combined with Beckstrom's Law, there is a way to put a cost on data breaches. Ponemon releases this report annually, reporting on different countries and geographical regions. Its organization is based on a per-capita, or per-record-lost cost basis: how much is a single PCI, PHI or PII record worth regarding breach cost? How does that vary per industry vertical?




The mean cost per capita for US companies in 2017 was $225. The probability of a breach that would carry a cost equivalent to a **10,000-record** loss in the United States is **27%** over the next 24 months – **28%** globally.

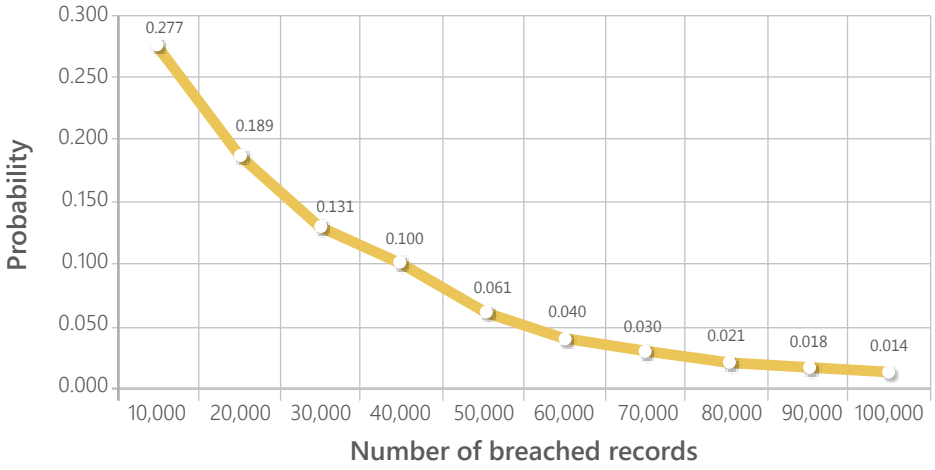
In short, there's a greater than 1 in 4 chance that your company will have an overall breach cost of **$3.62 million** in the next two years.



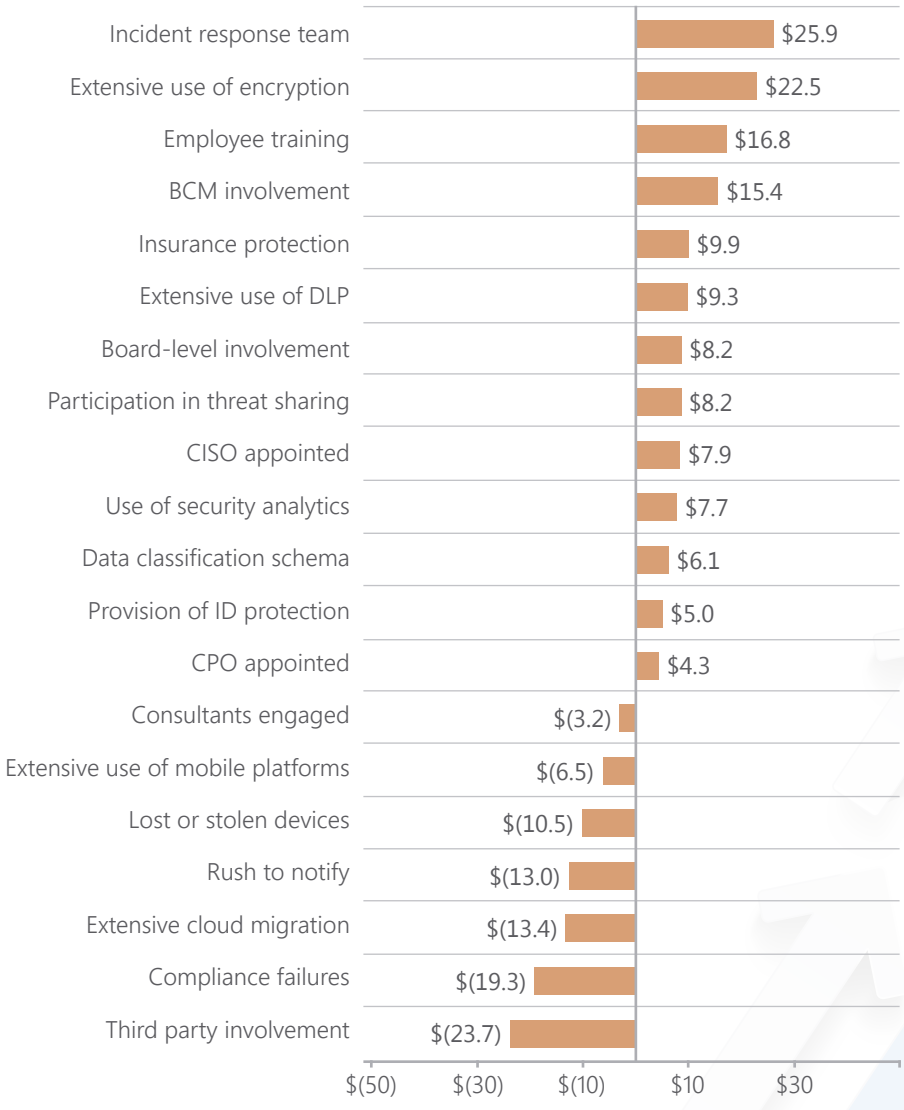

**27.7%**

Average likelihood of experiencing a breach of 10,000 or more records over a 2 year period

US in 2016: 24%
Globally 2016: 26%




But there's more, and this is the exciting part: the Ponemon Breach Cost Report includes figures for how much a breach cost is reduced by undertaking certain security initiatives. Per the graphic below, these activities reduce per-capita breach costs by the deviation from the mean of $225 as shown. Combining this with Beckstrom's Law is a wonderful way to illustrate ROI or ROSI.



It is vitally important, then, that security programs are fully developed and ready should a breach occur. Most security practitioners would agree that it is not a matter of if but when that may arise, with the hope that it has not already happened. Increasing capabilities in detection by using Managed Security Services to monitor and alert is a smart and effective way to resolve prevention bias: MSS starts up very quickly with little or no capital expense, establishes capable procedures immediately, is staffed with qualified personnel, and is likely to cost much less than it would if a company chose to build its own SOC.

Boards and security leaders can use these ROSI calculations when developing their strategic security plans. Combining these security initiatives can also greatly reduce the actual costs of the risks posed by security breaches. To maximize your ROSI, use Managed Security Services to handle your detection, alerting and even much of your incident response – **contact CIPHER** to find out how.

Founded in 2000, CIPHER is a global cybersecurity company that delivers highly accredited Managed Security Services and Security Consulting Services with ISO 20000 and ISO 27001, SOC I and SOC II, PCI QSA and PCI ASV certifications. We have received many awards including Best MSSP from Frost & Sullivan for the past five years. These services are supported by the best in class security intelligence lab: CIPHER Intelligence. Our offices are located in North America, Europe, and Latin America with 24×7×365 Security Operations Centers and R&D laboratories, complemented by strategic partners around the globe.

Our clients consist of Fortune 500 companies, world-renowned enterprises, and government agencies with countless success stories. CIPHER provides organizations with proprietary technologies and specialized services to defend against advanced threats while managing risk and ensuring compliance through innovative solutions.

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


**NORTH AMERICA**

703 Waterford Way
4th floor
Miami, FL 33126 - US
+1 305 373 4660

1 Glenlake Parkway
7th floor
Atlanta, GA 30328 - US
+1 404 877 9170

**EUROPE**

2 Kingdom Street
6th floor - Paddington
London - W2 6BD - UK
+44 203 580 4321

**LATIN AMERICA**

R. Alexandre Dumas 1658
2º andar - Chac. Sto. Antonio
Sao Paulo - SP 04717-004 - BR
+55 11 4501 6600