WHITEPAPER

Cyber Security: Beyond the Burden and Into Revenue

Your budget this year shows need for restraint. You've got to apply an intelligent strategy to the funds you do have. Because your basic cyber security has worked so far, you diagnose it as "good enough" and unworthy of the budget investment pool. And really, what are the chances of cyber hackers attacking your tech company? Also, cyber security is a one-way expenditure. Money goes in, but there's no return, right? Wrong.

YOU WILL LEARN:

- The average costs of a cyber breach
- What happens to most small businesses after a breach
- How strong cyber security can be seen as profit potential
- Why CEOs see cyber security as an investment opportunity

SUNGARD AVAILABILITY SERVICES

Assurance Software

The Cost of Not Investing

Commonly, areas of spending that don't directly or immediately affect productivity or profit get sentenced to the budget chopping block. And decision-makers often implicate cyber security in that line-up.

It's one area they see fit for corner-cutting and dollar saving. However, according to an IBM Security study, the financial damage of a cyber breach for a U.S. business hit an average of $7.35 million in 2017 — up 5% from 2016.[1] Of course, that figure can fluctuate depending on the organization's size and industry, and the nature of the attack itself. But even a small business can incur average damages between $84,000 - $148,000. And within six months of an attack, 60% of small businesses go under.[2]

With such significant loss potential, how can any company — large or small, in any industry, particularly the tech sector — look at cyber security only as an expense? The price you could pay for a cyber attack certainly exceeds the price of sturdy cyber security. And that is only looking at the immediate monetary damage. Succumbing to a strike also costs you your reputation, customers, and stakeholders — which sustains additional financial loss down the road.

$7.35 MILLION

Average damage of a **cyber breach** in the U.S. in 2017[1]

IN FACT 60%

Of small business go **under within 6 months** of an attack[2]

A Different View on Revenue

Perhaps some executives are finally accepting this reality. A recent survey conducted by KPMG's CEDO Outlook 2017 reported that 70% of CEOs now regard robust cyber security as a revenue opportunity rather than a burden, as in the past.

They realize advancing cyber technologies are pervading how and with what we do business, and that these modern tools and processes come with vulnerabilities that didn't exist even 10 years ago. Strengthening these weaknesses means safeguarding their company, customers, and finances. CEOs and other decision-makers are beginning to acknowledge that cyber terrorists are not rare specimen and that attacks are escalating.

Hackers Like U.S. Companies

Cyber criminals have managed to hack the U.S. into the number one position as the country with the most business data breaches — 1,579 in 2017.[3] Also to consider: this count represents actual breaches — meaning a system that was infiltrated and data compromised. This grossly overshadows 2016 stats with a 44% jump. It does not encompass *attempted* attacks that were shielded by ample cyber security. A 2016 State of SMB Cybersecurity Report states that 14 million small businesses incurred an attempted hack or a breach.

CYBER CRIMINAL MOS

- → *Network infiltration* and acquisition of data to sell
- → *Collection of ransom* for data held hostage
- → *Password theft* to gain access to financial & other data
- → *Delivery diversion* from customers to themselves

Sharing is Caring for CEOs

Additionally, CEOs are also accepting responsibility as participants of cyber security development and management, rather than delegating the entire mission. Cyber security knowledge no longer sits within the confines of IT. An executive's skillset now calls for basic cyber security aptitude. VIPs agree that a portion of their leadership role entails not only revenue generation, but also promotion and protection of their reputation, and trust in the business. They are now conceding that cyber security — or lack thereof — falls under that umbrella as it directly affects all three.

CYBER CRIME STATS

$2 MILLION

Cost of cyber crimes expected by 2019

Symantec predicts *smart device attacks* will increase in 2018

7.8 BILLION

Records were compromised by breaches in 2017

Largest cyber breach to date: Yahoo with 3 billion user accounts affected

The Dollars & Cents of a Cyber Breach

Still, some execs can't fathom the cost of an attack. But translating a breach into dollars can help them grasp the potential loss.

1 Business Disruption

This includes process and service disruptions, and compromised employee productivity — ***consuming up to 39% of total external costs.***

2 Compromised Records

Each U.S. record jeopardized tallies around $225.[5] Multiplying that by a few hundred, ads up stiffly; raise it by a few thousand records, and it can be a debilitating debt.

3 Customer Loss

In 2016, Vanson Bourne, a technology market research specialist, conducted an independent study finding ***76% of those surveyed would cease association with a breach-prone business.*** Once customers feel their information is not safe with you and/or they cannot rely on you for steady service, they will jump ship.

DISRUPTION STATS

$21,155 / DAY

Average daily cost of downtime

46 DAYS

Average resolution timeframe

$973,130

Average total disruption loss

4 Legal Dues

It's not uncommon for a company that has sustained a cyber breach to also get knocked with *a class-action lawsuit.*

5 Regulatory Fines

The Federal Communications Commission (FCC), Payment Card Industry Data Security Standard, Federal Trade Commission (FTC), Health and Human Services — and host of other agencies — can delve out *fines to add to your breach debt.*

6 Direct Monetary Depletion

If hackers gain access to financial records or accounts, they're free to take what they please, possibly *draining your funds.*

7 Public Relations (PR) Costs

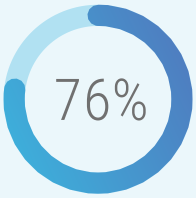
PR may need to be rallied to *repair your reputation.* And many states mandate companies to notify those affected by a breach.

$10 MILLION

Paid by major orgs. for **legal ramifications** of breaches

$500,000

2016 average cost of **breach alert to affected customers**



of those surveyed **would cease association** with a breach-prone business.

“If hackers gain access to financial records or accounts, they're free to take what they please, possibly draining your funds.

The Revenue Wrap Up

When broken down to individual expenses, it's easier to read a cyber breach on the liability side of the ledger. The assumed immediate savings of cutting cyber corners exposes you to greater long-term loss inflicted by an attack. A dedicated business analysis within a comprehensive business continuity plan (BCP) can help bring to light your company's specific risks and potential costs of a breach.

A breach actually is a cut in revenue not only for monetary loss, but also the trust, consumer confidence, data, trade secrets, and downtime it steals. Investing in well-built cyber security methods will yield steady operations for sustained revenue opportunities, and bolster trust within your customers and business associates to keep them spending with you. Cyber security is revenue security.

ABOUT ASSURANCE SOFTWARE

Assurance Software takes your company's enterprise-wide business continuity and resiliency program to the next level. Assurance Continuity Manager and Assurance Notification Manager work together to help your company increase efficiencies, mitigate risk, and safeguard what you value most. From Incident Management that allows your business to manage recovery seamlessly to business impact analysis' that are customized to your needs — Assurance protects every aspect of your business.

1. *Ponemon Institute's 2017 Cost of Data Breach Study, IBM Security, 2018 https://www-01.ibm.com/common/ssi/cgi-bissialias?htmlfid=SEL03130WWEN&*
2. *USA Today, Cyber Threat is Huge for Small Business, 2017 https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/*
3. *IT Security Central, Cyber Security Statistics 2017: Data Breaches and Cyber Attacks, 2018 https://itsecuritycentral.teramind.co/2018/01/03/cyber-security-statistics-2017-data-breaches-and-cyber-attacks/*
4. *Data Breaches Cost Businesses an Average of $7 Million, Business Insider, 2017 http://www.businessinsider.com/sc/data-breaches-cost-us-businesses-7-million-2017-4*
5. *Sfax Secure Fax, The Average Cost of Data Breach in 2017, 2017 https://www.scrypt.com/blog/average-cost-data-breach-2017-3-62-million/*

For more information on business continuity for the technology industry and how Assurance Software can help you maintain compliance, contact a certified business continuity professional.

WWW.ASSURANCESOFTWARE.COM