The Value of Documented Cybersecurity

Leveraging Proactive Documentation as a Cost-effective Solution

DAYBLINK

Introduction

The latter half of this past decade saw a record number of cybersecurity failures. The biggest breaches had headline-grabbing impacts and heavy financial costs. In 2017, The Equifax hack exposed the personal information of 143 million consumers, and Equifax itself lost $4 billion in stock market value by that September. The WannaCry ransomware attack created $4 billion of damage to business operations in over 100 countries. The Petya / NotPetya ransomware attack that closely followed WannaCry had dire effects on the operations of FedEx and Maersk and a total estimated cost of $300 million. This was the emergence of a new era, and the trend continued unabated. In 2018, Marriott announced 500 million travelers had their data compromised, and the city of Atlanta was struck by a crippling ransomware attack. In 2019, a Quest Diagnostics breach exposed 11.9 million patients' medical and financial data, leading to the bankruptcy of the American Medical Collection Agency (the contractor found to be at fault). In 2020, even after their 2018 compromise, Marriott announced another breach of 5 million users' personal information. These are just a few examples.

The cost of cybersecurity losses, however, was not limited to hundred-million-dollar sums and multinational corporations. Staggering financial losses hit enterprises and small businesses alike, at an average loss of $1.3 million per impacted enterprise and $117k per impacted small business. This widespread impact is part of an accelerating trend in worldwide cybercrime that is expected to cost the global economy $6 trillion by 2021 - a full double its impact in 2015. These figures aren't the result of sporadic or unpredictable events that only impact major corporations - more than half of all U.S. businesses were hacked in 2017 (54%), which has increased to 67% in 2019. This a global surge in cybercrime and corresponding cybersecurity spend.

As can be expected, a great deal of industry excitement has resulted. Fair warning: this paper does not discuss exciting or trendy cybersecurity platforms or applications. This is the single most boring aspect of security...the paperwork.

Discerning executives with limited budgets must sift through the multitude of legitimate and illegitimate cybersecurity offerings and choose defensive tools wisely – minimizing the risk of a cybersecurity breach, the resulting costs, and the cost of protection. Doing so requires a thorough understanding of the following factors:

1. Cybersecurity breach threat vectors – what are the avenues of potential attack?
2. Cybersecurity breach cost drivers – what causes financial loss when a breach happens?
3. Cost-benefit analysis of solutions – do solutions address both threats and cost drivers?

The most foundational cybersecurity solution that addresses both threat vectors and cost drivers of security breaches is proper documentation.

The greatest cybersecurity threats come from human error and lax vulnerability management, which can be remedied through proper employee training and an efficient, standardized approach to vulnerabilities. Training and standardization programs are borne of properly documented security policy and procedures.

The largest cost drivers of security breaches are legal liability. Anthem, Inc. paid $115 million to settle class-action lawsuits regarding a data breach of 79 million customers, while Target paid over $200 million due to regulatory fines, legal fees, and class-action settlements. Properly documented security policy and procedures is proof of compliance and competence, and minimizes legal costs. It demonstrates to auditors, courts and witnesses that everything reasonable was done before the breach.

Threat Vectors

Identifying the attack vectors of cybersecurity threats is the first step towards effective remediation. Documentation of those threats, including how they may impact critical systems or data, ensures that they can be understood organization-wide. In a survey of enterprise corporations (1000+ employees), respondents named cybersecurity threat vectors that were expected to have the most dire financial consequences. The results of these surveys are helpful in identifying threat vectors that need to be both documented and addressed by effective countermeasures.

Threat Vector	Cost per Incident
Physical loss of devices or media containing data	$2.8m
Third-party IT infrastructure incidents	$2.2m
Electronic leakage of data	$1.9m
Inappropriate IT use by staff	$1.1m
Viruses and malware	$519k

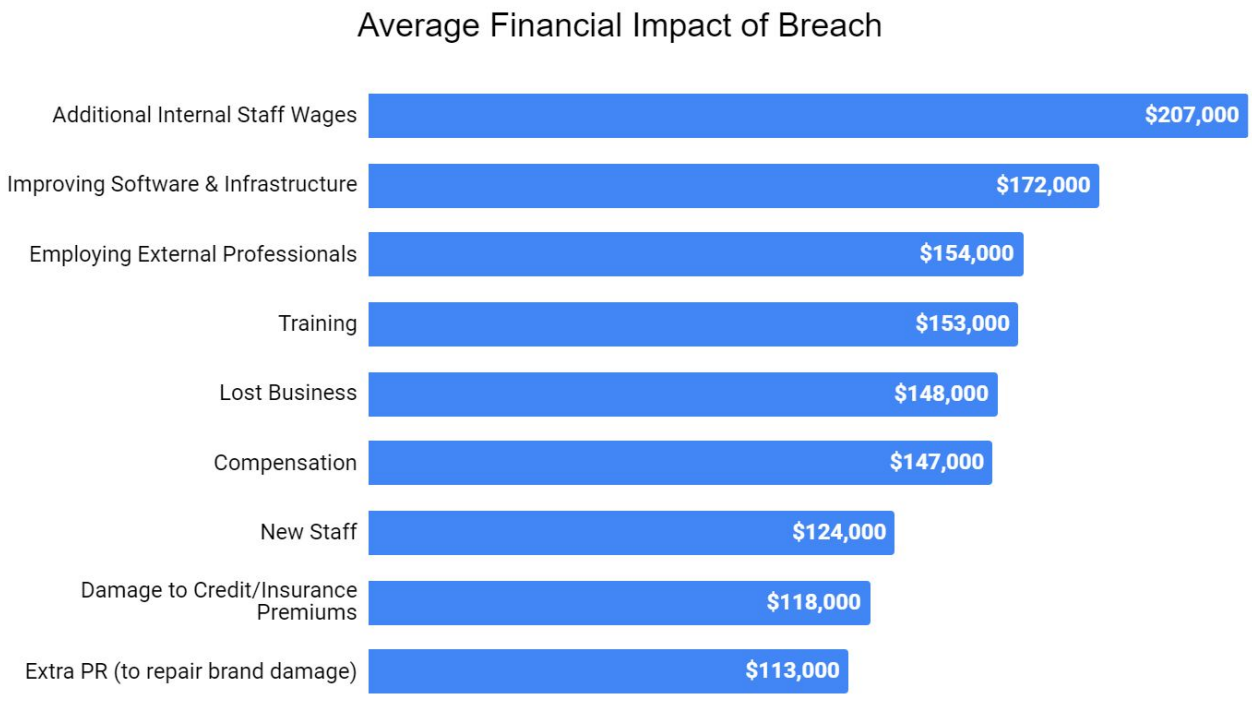
Tables sourced from industry-expert interviews, research and analysis

There are a few key takeaways from this data. Firstly, viruses and malware alone are the lowest priority for cybersecurity protection of any business – meaning that it is individual mistakes, partnerships, and internal threats that pose the greatest financial threat. An employee losing their phone may breach IP or leak a new prototype accidentally (as has happened with multiple Apple releases). A third party may have insufficient redundancy measures and lose critical data. An employee may inadvertently install malware or misuse company resources. These are not technical flaws – they're human ones.

Cost Drivers

Once the threat vectors have been identified, it is critical to address the costs resulting from successful compromises of a system (regardless of how effective countermeasures are, it is prudent to assume that mistakes will be made and breaches will occur). The countermeasures that should be given the greatest priority are those which both limit the number of breaches as well as the impact of successful breaches.

In a study conducted of businesses who had been breached within the past 12 months, businesses with 50 or more employees were asked to estimate the costs they incurred in specific categories, then differentiated their results once more between SMBs and Enterprise organizations. The graph below shows the aggregated cost estimates of both categories.



Tables sourced from industry-expert interviews, research and analysis

For enterprises, the improvement of software and infrastructure post-breach, in addition to improvements to cybersecurity staff, were the largest cost drivers. This is arguably due to the necessary replacement and upgrading of compromised or vulnerable systems, and the replacement or augmentation of existing cybersecurity teams. External professionals were also costly.

How, then, can these overall costs be minimized?

- The cost of training new cybersecurity hires can be lowered, and standardized, by creating role descriptions in line with security policies and specific procedures. These can also be referenced as proof of employee qualification requirements in the event of a cybersecurity breach.

- Baseline security configurations and network maps for damaged assets will reduce time and effort when bringing new systems online in the aftermath of an attack. These further ensure that once those assets are properly functioning they do not expose new or unexpected vulnerabilities – and that they function as intended.

- External professionals should be a one-time cost when establishing policies, rather than an expensive cleanup crew in the aftermath of a disaster. Those policies can serve as a reference point during cybersecurity crises.

Costs and Benefits of Documentation as Support and Solution

It is undeniably a business cost to establish thorough information security policies and standards for any company. The development of these documents takes employee time away from revenue- or production-based activities, requires centralized coordination, legal and management approval, and a schedule of regular review and update. This cost, however, is much lower than the cost of an effective cybersecurity breach. Documentation is uniquely able to both proactively limit threat vectors and minimize the costs of a breach after the fact.

As has been outlined, the most severe threat vectors result from human error and lax implementation. This can be proactively guided by policy and procedure documentation. Data storage and handling policy, backup procedures, appropriate use policy, encryption standards, and third-party contractual agreements are all proactive documents that guide interaction with the most critical aspects of any business' information security domain. Proper employee training, utilizing the information in these documents, limits the potential for mistakes that result in major cybersecurity breaches.

After a cyberattack, cybersecurity baseline documents like hardened asset configuration schematics and network maps can reduce downtime and the cost of replacing damaged or vulnerable systems. But the documents that attempted to prevent the breach have additional purpose – that of limiting legal and public liability. Thorough documentation of a reasonable cybersecurity approach can prove to auditors, courts, and the general public that a company was not at fault, but rather a victim. This can mitigate the loss of fortunes in civil lawsuits - as noted previously, Anthem Inc. and Target lost hundreds of millions on class action lawsuits and regulatory fines.

Of the cost drivers listed for enterprises post-breach, effective documentation can contribute to minimizing legal costs, train new staff, minimize insurance costs, and provide configurations for software and infrastructure replacement. Whether the cost of creating and maintaining documentation is financially justified can be determined through a basic Return on Investment (ROI) analysis.

As established, the average enterprise loss from a successful cyberattack is around $1.3 million. This can be considered the single loss expectancy of a cyberattack. Assuming there are 12 successful cyberattacks per year (one per month on a corporation without proper security measures - a conservative figure, as most CISOs are aware), the annualized loss expectancy becomes $1.3m X 12 = $15.6m. This is an appropriate budget limit for an enterprise corporation to spend on all cybersecurity measures (on average). While this may seem like a large number, it is important to remember the immense sums that Equifax, Target, Anthem, Yahoo!, FedEx, and Maersk all lost due to breaches (hundreds of millions).

But what about documentation specifically? According to the Aberdeen Group and Wombat Security, proper awareness training, which relies on documentation, can reduce the risk of cyberattack by 45-70%. Having observed industry-wide a conservative average of a 50% reduction, that's $7.8 million saved due to training and awareness based on the annual loss expectancy of $15.6m. Conservatively, if documentation accounts for just 25% of training and awareness, then it contributes $1.8 million in risk prevention annually. That's without estimating the post-breach benefits of documentation in cost reduction.

The categories of post-breach loss that documentation addresses - legal costs, new staff training, insurance losses, and software/infrastructure configurations - come to a total approximate impact of $597,000 out of the $1.3 million average cost of a single cybersecurity breach, per the IT Security Risks survey previously referenced (See table on next page). Thus, the annual loss expectancy from post-breach losses that can be directly addressed by documentation comes to $6.8 million.

Qualitatively, the process of documenting cybersecurity policies and procedures can help to refine and improve security behaviors by building consensus within a team. Documentation can also provide for avenues of support in a crisis, where IT employees are re-assigned, or rapid shifts in scheduling can be pre-planned.

Clearly, documentation cannot totally eliminate expected costs, but several years of history across many different clients have clearly demonstrated that the end results have saved our clients as much as $3 million in cybersecurity breach and breach cost avoidance annually.

Cost Driver	Documentation	Savings Per Incident
Infrastructure	Secure Configurations	$172,000
Legal Costs	Cybersecurity Documentation	$154,000
Staff Training	Standard Procedures	$153,000
Insurance Losses	Robust Policies	$118,000
Team Organization	Documentation Procedure	$130,000 (~10% of breach loss)

DayBlink has quantifiably reduced the potential for losses by improving procedures and creating documentation, which then improves employee training and awareness. By increasing training and awareness based on centralized documentation and standardized procedures, clients completely prevent as much as $1.8 million in cybersecurity breaches per year. For those remaining breaches that still occur, documentation continues to play a role in addressing post-breach cost drivers (the annual expectancy of which is reduced to $5 million due to breach prevention). That ongoing role limits legal fees, training, insurance, and configuration losses by as much as 50%, or $2.5 million. Highly conservatively, if documentation only limits post-breach losses by 25%, it contributes $1.25 million in loss prevention.

Given these quantified amounts - $1.8 million in breach prevention and $1.25 million of post-breach cost reduction based on the most conservative perspectives, we can calculate ROI of an investment in cybersecurity documentation. A thorough enterprise-level documentation of cybersecurity procedures that addresses training and standardization can cost between $500,000 - $1m depending on the complexity of the organization.

$3.05 million of cost avoidance / $750,000 cost = ~400% ROI

This figure is based on the most conservative estimates of documentation contributions to training and awareness, breach prevention, and cost remediation post-breach. It assumes that the proper documentation of training and awareness programs only contributes 25% of their value, and that having documented evidence of cybersecurity due diligence and best efforts will only reduce legal costs 25% after a breach (both figures are in reality much higher).

Documentation is an essential cybersecurity step that supports a properly rigorous cybersecurity posture. It can address the largest breach cost drivers at a fraction of the cost of other preventative measures. Most especially, it can reduce legal and PR cost by demonstrating a proactive cybersecurity stance, while building a team understanding of proper security behaviors. Failing to plan is planning to fail, and most companies cannot afford such a loss.

Tables sourced from industry-expert interviews, research and analysis

REFERENCES

1. Fulford, Mark. “4 of the Most Expensive Cyber Attacks of 2017 (and How They Could Have Been Prevented)” LBMC Information Security, Oct. 2017: https://www.lbmcinformationsecurity.com/blog/4-of-the-most-expensive-cyber-attacks-of-2017-and-how-they-could-have-been-prevented

2. Lim, Paul J. “Equifax’s Massive Data Breach Has Cost the Company $4 Billion So Far” Money Magazine, Sept. 2017: http://time.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/

3. IT Security Economics Report. “IT Security: Cost center or strategic investment?” 2017: https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Econmics%20Report%209.18.17.pdf?aliId=500849643

4. Morgan, Steve. “Cybercrime Damages $6 Trillion by 2021” Oct. 2017: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

5. Hartford Steam Boiler Inspection and Insurance Company (HSB), subsidiary of Munich Re. “Half of US Businesses Have Been Hacked” Sept. 2017: https://www.munichre.com/HSB/business-hacked-survey-2017/index.html

6. Crowe, Jonathan. “10 Must-Know Cybersecurity Statistics for 2018” Feb. 2018: https://blog.barkly.com/2018-cybersecurity-statistics

7. DiGiacomo, John. “The High Cost of Data Breaches: Six Examples from 2017. Revision Legal, March 2018: https://revisionlegal.com/data-breach/cost-of-data-breaches/

8. Wombat Security. “New Research from Aberdeen Group and Wombat Security Confirms Security Awareness and Training Measurably Reduces Cyber Security Risk.” Jan. 2015: https://www.wombatsecurity.com/press/press-releases/research-confirms-security-awareness-and-training-reduces-cyber-security-risk

ABOUT THE AUTHORS

Steven Nyikos, CISSP, is a Senior Consultant within DayBlink's Cybersecurity Center of Excellence

Michael Morgenstern is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence and is based in Boston, Massachusetts

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cybersecurity@dayblink.com
Call: 1 (866) 281-4403