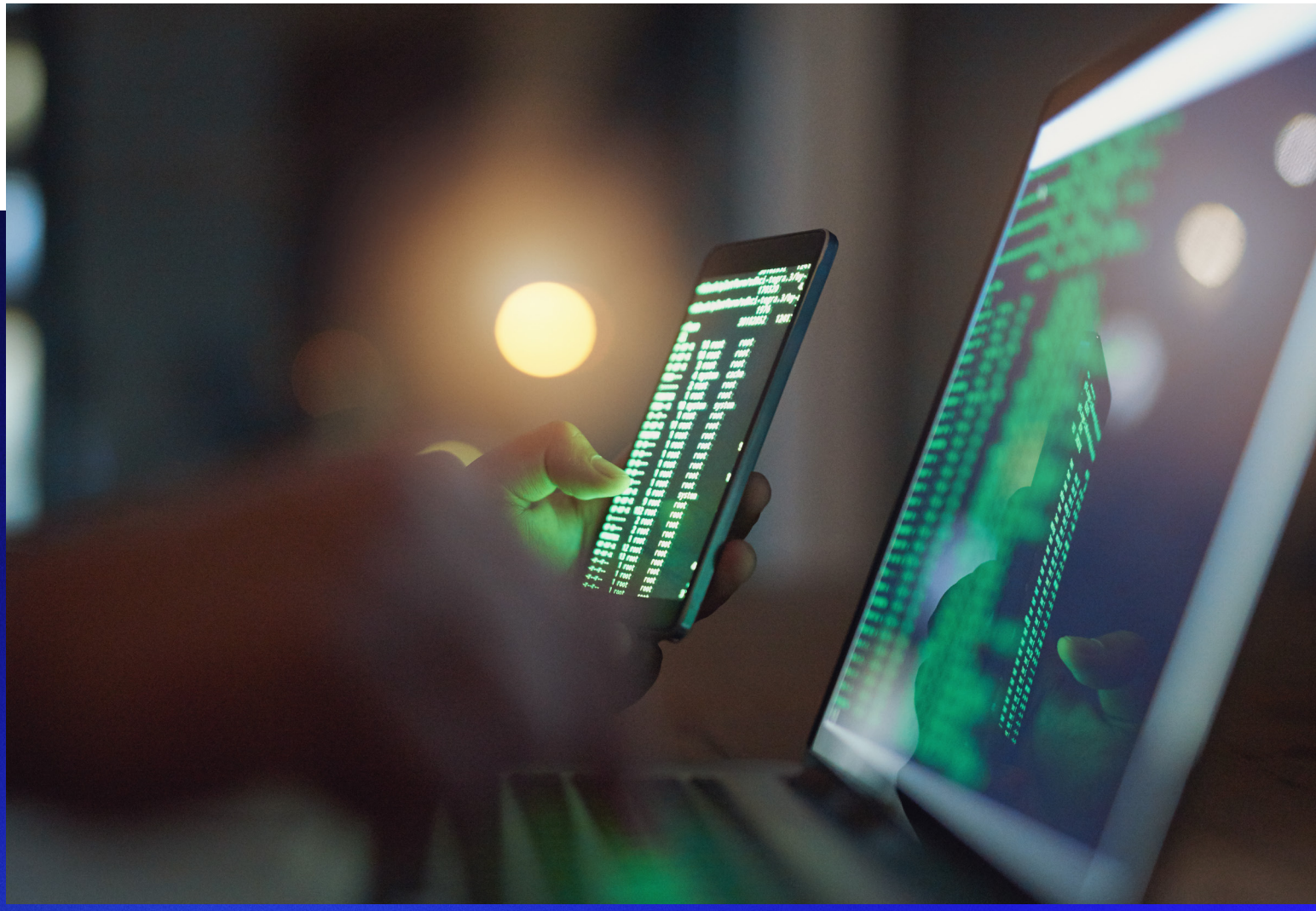
Secureworks®

WHITE PAPER

The Cost of Making the Front Page: What You Need to Know About the Growing Threat of Public Breaches



The headline cost of falling victim to a cyberattack is rising. Following a late December 2019 breach, Travelex, a London-based foreign currency exchange allegedly paid the ransomware operator $2.3 million USD[1]. In April 2020, a U.S. law firm faced a ransom demand of $21 million, later rising to $41 million.[2] Typical ransom demands just three to four years ago were closer to $10,000.

It's no secret that ransomware demands are getting larger, but that's not the only type of attack resulting in spiralling costs for victim organizations.

Some estimates suggest that the overall cost to British Airways of the breach disclosed in September 2018 may reach $1 billion USD. That attack did not involve data encryption or ransom demands. Instead it saw cybercriminals using third-party code on the BA website to divert customers to a fraudulent site where personally identifiable data from as many as 500,000 customers and approximately 380,000 credit card numbers were captured.

These other costs fall into multiple categories and have short and longer term impacts. Some, such as loss of business or reputation and trust, are more theoretical than others, but breach planning involves an element of risk calculation and it is worth considering the possibility of worst-case scenarios.

Clearly, a ransom is not the only cost associated with a public data breach. In fact, other cost elements can be so significant that the ransom is often only a fraction of the total cost incurred.

Operational and Technical Costs

In the immediate aftermath of a breach, organizations may be faced with business systems that are partially or even entirely compromised. Business operations may be impacted or even halted completely, with corresponding impacts on revenue generation. The initial priority is to determine the extent of the incident and the damage caused, to evict the threat actor, and to remediate wherever possible so the organization can get back to work.

Operational and technical costs will vary, depending on the type of breach and whether systems are partially or fully compromised and the degree to which technical recovery is required. At the very least, system recovery will consume existing internal technical resources, diverting them from normal responsibilities. The victim may need to engage and pay for external, expert incident response services.

Ransomware, particularly if backups or the decryption key are not available, may require more intensive technical resources for remediation than other types of breaches.

Call center costs may rise as customers find themselves unable to access services. Processes may need to be carried out manually, requiring an increased temporary headcount. In the wake of the Travelex breach, Travelex had to take down its systems across 30 countries and revert to working with pen and paper until it was able to start restoring systems two weeks later. Some of its websites remained offline over a month after the attack.

[1] BankInfoSecurity, Travelex Paid $2.3 Million to Ransomware Gang: Report

[2] Computer Weekly, Law firm hackers threaten to release dirt on Trump

Indeed, the entire business is likely to be affected in cost-bearing ways that go far beyond system access. There will be impacts on legal, marketing, customer services, public relations, and more. External, fee-bearing assistance will often be needed from highly specialized external advisors, for example in crisis management or computer forensics.

$7,500

USD was charged against each voilation which means $7,500 per incident, per consumer under CCPA.

Regulatory Costs

Regulatory fines may come into play if personally identifiable data has been disclosed. In many jurisdictions, organizations are now obliged to disclose breaches within a very limited timeframe.

Since GDPR came into force, the size of regulatory fines has increased dramatically, adding to cost burdens. The U.K.'s Information Commissioner's Office (ICO) stated that it planned to hit BA with a record fine of £183 million ($234 million USD).[3] That compares to a pre-GDPR maximum fine of £500,000 imposed on Cathay Pacific for a breach that leaked the personal details of 9.4 million customers.

The penalty imposed on BA for what the ICO called "poor security arrangements" could have been even higher. It equated to around 1.5% of annual revenue at the time for BA, but the maximum permissible fine under GDPR is 4%.

Fines under the California Consumer Privacy Act (CCPA) could hit $7,500 USD for each violation which means $7,500 per incident, per consumer. For a breach the size of BA's, that would greatly exceed the GDPR fine.

Enterprising ransomware operators are taking advantage of this prospect by using the risk of regulatory fines as a threat to encourage victim organizations to pay the ransom promptly. Failure to pay results in the victim's name being publicized on the threat actor's leak site.

Customer Costs

The requirement to notify customers that their data may have been disclosed has another potential financial impact, in addition to fines. It gives customers the ability to take action to protect themselves by changing passwords, but it also leads to compensation demands and class action lawsuits:

- Equifax agreed to a global settlement after the breach announced in September 2017 that included up to $425 million USD to help people affected by the breach.[4]
- Walmart has been sued in a class action suit allowing personal information to end up on the dark web after an undisclosed data breach.[5]

[3] Information Commissioner's Office, Intention to fine British Airways £183.39m under GDPR for data breach

[4] Federal Trade Commission, Equifax Data Breach Settlement

[5] Top Class Actions, Walmart Class Action Lawsuit Says Customers Subjected to Data Breach

- A class action lawsuit against BA has been allowed to go ahead. Signup for customers closes in January 2021 and the eventual bill could exceed the GDPR fine.[6]

On top of the settlement costs, attorney fees and litigation expenses are incurred. In addition, the processes required for customer notification adds another layer of cost.

Loss of Business

How a breach causes an organization to lose customers depends on the nature of the breach and the organization itself. Downtime for an e-commerce website may lead to consumers with an immediate requirement for a specific purchase to quickly search for another retailer, resulting in a number of lost sales. While the cause of the hour of downtime Amazon experienced on Prime Day in July 2018 is not clear, estimates suggest the cost reached $100 million USD in lost sales.[7] Lost customers may not return. British bank TSB's IT problems in 2018, while not attributed to a breach, are estimated to have lost it 80,000 customers.[8]

Larger corporate customers may not be able to switch suppliers quickly but may be more hesitant to renew contracts. Three weeks after the Travelex breach, banks and supermarkets using its white labelled foreign exchange services were still facing disruption to their own operations. Either way, revenues are lost.

Another impact of regulation is that it's no longer possible to keep breaches quiet. So, in the short term, customers could be lost, not just because system unavailability means services cannot be supplied, but also because clients no longer trust the business with their data or money.

This isn't limited to immediate business either. An inability to kick off or move into a new phase of an engagement on a specific date may lead to a contract not being signed or a break clause triggered, with the business and revenue going to a competitor.

In the longer term the impact can even potentially affect an organization's market position.

Loss of Reputation and Trust

Longer term impacts of breaches on organizational performance can be hard to assess in isolation. Both British Airways and Travelex, for example, have also been severely impacted by the COVID-19 epidemic. However, particularly in cases where an organization has been unable to supply services for a significant period, it could be challenging and expensive for it to regain its former market position. The value of the brand and other intangible assets could be damaged, impacting balance sheets.

---

[6] Lawyer Monthly, BA Back Down on Data Breach Claim Window

[7] Business Insider, Amazon's one hour of downtime on Prime Day may have cost it up to $100 million in lost sales

[8] Independent, TSB IT meltdown cost bank £330m and 80,000 customers

An organization could lose not only customers but its position within supply chains. Suppliers might hesitate to deal with an organization that has demonstrated a lack of care in how it treats partner data or has shown itself to lack the resilience to continue operations during the aftermath of an attack.

If IP has been stolen in a breach, competitors may be able to catch up on market position by improving their offer, further reducing income. IP theft is estimated to cost U.S. companies as much as $600 billion USD a year.[9]

Small company breach victims could even go out of business.

There are other potential costs too: insurance costs are likely to rise in the following year. It may be necessary to raise capital finance to compensate for a loss of revenue.

If a hidden attacker isn't fully evicted from a system after a successful attack, it could all happen again, with another round of short-term costs for weeks or months after. Australian brewer Lion was hit with two ransomware attacks in short succession in 2020.

Understanding the Risk and Being Prepared

There's no escaping the fact that today, organizations may have to deal with breaches in the public eye. These multiple potential costs, some more certain than others, emphasize the value of being prepared and of security policies that highlight the importance of monitoring and detection.

While some attackers are undoubtedly skilled, many breaches happen because of basic security oversights. Some breaches are made worse by a lack of both foresight and of planning for incident response and stakeholder crisis communications.

It is vital for business leaders to understand the potential consequences of a breach, both in the short and longer term. The answer is to be prepared. Both financial and reputational costs can be reduced with proper preparation and an informed, rehearsed response. Where appropriate, transparency and moving swiftly to a prepared response can even gain an organization public credit.

That means senior leadership, not just the security team, must understand the risk associated with a public breach.

Secondly, the practical aspects of the organizational security stance must be well understood, especially where it may fall short.

Finally, leadership needs to understand that few organizations can count on escaping the attention of opportunistic cyberattackers. For that reason alone, it is wise to prepare for a breach. All organizations need an incident response plan and a messaging strategy rehearsed and in place.

[9] CSO, Intellectual property protection: 10 tips to keep IP safe

Conclusion

Organizational cybersecurity decisions can only be taken within in the context of the corporate business risk profile. How the business responds to a breach and, in the case of ransomware, whether it decides to pay the ransom are business risk decisions. However, the broad array of potential cost elements and the possibility of long-term damage make it imperative to realize the importance of the right preparation.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp