BISHOP FOX | timehop

How ‘Small’ Security Errors Lead to a Security Breach

One simple cybersecurity error can lead to
a costly security breach.

FOREWORD:

How this Collaboration Between Timehop and Bishop Fox Came to Fruition.

When Timehop learned that they had been breached on the first week of July 2018, their approach to addressing the aftermath was uncommon. More often than not, breaches are treated like the awkward elephant in the room – yes, they exist, but let’s not dwell on the details. Timehop turned this approach on its head.

Bishop Fox has decided to publicly support Timehop and their commitment to transparency. In the following document, we discuss several pervasive security errors we have seen in our work and how they have led to serious consequences for many organizations (including Timehop). In turn, Timehop also has contributed a case study on what exactly went down in the hours following news of their breach.

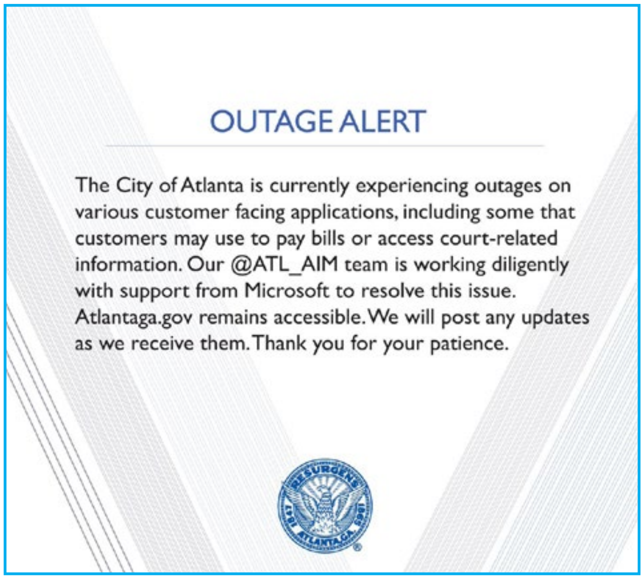
We hope this document can serve as a guide of how your organization can refrain from falling for the same errors.

Bishop Fox Guide - V1, Updated July 2018 - A.D.

CYBERSECURITY ERRORS GUIDE

INTRODUCTION

The City of Atlanta operates under a $650 million budget and provides municipal functions for close to a half-million people. And in one day, because of a cybersecurity error, nearly half of the city’s 13 local departments were disrupted by a ransomware attack that prevented those agencies from collecting revenue, citizens from receiving services, and left records and data crucial to law enforcement and government operations inaccessible. In the end, Atlanta may spend up to $2.6 million on costs related to this security breach, including incident response, system recovery, and crisis management.



OUTAGE ALERT

The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.

It’s a familiar refrain, regardless of the scale of the attack. Rarely are enterprises and smaller businesses taken down by APTs armed with zero-day exploits. Instead, malicious activity such as this thrives on the too-chilling reality that IT admins and network operators are swamped with day-to-day realities of their jobs, and as a result, things fall through the cracks. Conversely, threat actors have the luxury of waiting to pounce on a weak or known default password to own a critical system, or it’s a missing patch too far down on the to-do list that takes down an organization.

THE CITY OF ATLANTA ISN’T ALONE IN THIS.

Atlanta isn’t the only cautionary tale here when it comes to real and present danger of small cybersecurity errors. How many thousands of organizations failed to deploy a Microsoft SMB v1 patch that had been available for months before the May 2017 WannaCry outbreak? How many connected DVRs and security cameras still had lousy default passwords guarding access to those devices that were exploited in the Mirai attacks of 2016?

Behind each incident are reasonably simple security errors that were made, or priorities that hadn’t been addressed, yet the consequences were severe. For shipping magnates A.P. Moeller-Maersk, the NotPetya wiper malware attacks—with its roots in the same missing SMB v1 patch at the heart of the WannaCry attacks—led to earnings losses between $200 million and $300 million in the summer of 2017. A.P. Moeller-Maersk’s recovery costs included rebuilding 4,000 servers, 45,000 endpoints, and 2,500 applications, which is close to its entire IT infrastructure. Pharmaceutical giant Merck also took months to recover from NotPetya and cited disruptions to manufacturing, operations, and sales worldwide.

TRANSPARENCY IN A STICKY SITUATION.

Timehop, the popular social media aggregator, is a case study in transparency and corporate integrity in such sticky situations – the mistake that they made (a lack of multi-factor authentication) was simple enough to sidestep, but they have been quick to admit their slip-up and take the proper steps to remediate the damage done. You’ll find more detail on their approach to incident response in the case study on page 6.

THESE ARE MORE ALIKE THAN YOU REALIZE.

There are commonalities among these incidents in that basic security approaches such as vigilant patching, improved password policies and enforcement, and regular and accessible backups—all within the financial and operational reach of most businesses—could have kept organizations clear of trouble. Here’s a deeper look at some of these avoidable cybersecurity errors:

CYBERSECURITY ERRORS CULPRIT #1:

POOR PASSWORDS

Admins and network engineers may be overwhelmed putting out day-to-day fires that lead to a security breach. End users, meanwhile, are flooded with their personal misery: passwords. Between their personal and business passwords, on average, people need to remember authentication for 25 business and personal applications and services. Therefore, it’s inevitable that users take shortcuts to do their work, download apps, and play games. That means using easy-to-remember, guessable passwords, and subsequently, passwords that are reused over and over across numerous services. One massive password breach can unlock users’ accounts across the web.

How to Break the Cycle. You may already have mumbled under your breath, “password manager.” And yes, that’s a valid recommendation, but it’s not a foolproof way to sidestep a password-related security error. You can have a password manager that contains nothing but poor passwords, and the purpose of it is then defeated. Also, password managers will reduce the number of passwords that users must remember, but the managers themselves are protected by passwords and users still need to select strong passwords to protect the contents of the managers.

In many cases, multi-factor authentication (MFA) is a dependable solution to prevent losses due to weak passwords. When attackers successfully crack or guess passwords, they will lack the additional factor required to complete the authentication process as the victim. Setting up MFA is becoming more mainstream, with sites from Gmail to Facebook now implementing it. Usually, all your employees will need to do is enter their password and hit a push notification on their phone. An easy enough way to mitigate another one of these disastrous cybersecurity errors.

CYBERSECURITY ERRORS CULPRIT #2:

LACK OF MULTI-FACTOR AUTHENTICATION

A lack of MFA might not be the direct culprit, but it is certainly an enabler. In today’s world, MFA is a well-known and highly effective security solution; and frankly, a necessity if you are handling sensitive information. This being said, MFA is still surprisingly uncommon in organizations. A study from 2017 revealed that 62 percent of small to medium-sized organizations have yet to implement MFA. In addition, several high-profile breaches in recent years – from the infamous Chase breach of 2013 to the more recent case of Deloitte –could have been prevented with proper MFA.

In the case of the 2017 Deloitte breach, their email database as well as all administrator accounts were compromised and sensitive client information was left exposed. All in all, 350 clients were affected by the breach. MFA could have prevented the breach.

With Timehop, MFA would have been instrumental in preventing their breach from materializing in the first place. Unfortunately, they lacked MFA on a critical administrator account. Timehop, however, has since implemented authentication on all its internal systems.

How to Break the Cycle. Install an MFA system – but don’t do it haphazardly. Improperly implemented systems can cause significant damage as well. And do not make the mistake of viewing MFA as a panacea; that’s simply not the case. It’s a proactive measure that can lessen risk of a compromise via weak credentials.

MFA has two major flaws: It can be bypassed if not set up properly and your employees may suffer from “security fatigue” when it comes to checking repeat notifications. They may erroneously verify a push notification that was actually sent by an attacker. Do your due diligence when selecting an MFA solution and ensuring it is set up correctly. In today’s security landscape, though, MFA’s benefits far outweigh its flaws.

CYBERSECURITY ERRORS CULPRIT #3:

SOCIAL ENGINEERING

Many successful online scams or malware attacks have their origin in convincing spams or phishing emails. Spam and phishing are still viable because social engineering works against the age-old weakest link: people. No matter how much awareness training organizations provide, people are going to click on links from spoofed sources, and believe that they're on the website they meant to be on. Social engineering is becoming a science and attackers have mastered how to replicate banking pages, write corporate messaging, and embed attacks in email attachments. They attain access to even the most sensitive of networks.

How to Break the Cycle. These are relatively simple and low-tech issues that can be addressed with a proper mix of policy and technology in order to avoid making a devastating cybersecurity error. For starters, don't expect all employees to become security experts. Security isn't their responsibility, nor should it be. Instead of investing exclusively in security awareness training, your IT department should be practicing proper network segmentation (so that if one account is compromised, it can do limited damage) and setting up users with only the minimum amount of permissions needed to do their job.

Your IT department needs to step up. Ensure that your organization's domain is not vulnerable to email spoofing, which enables attackers to create emails that look like they're coming from inside your network, something that simplifies phishing attacks.

Awareness training still has its place; training should not only teach users how to spot suspicious messages, and not click on attachments, but also work closely with IT and encourage them to communicate suspicions and contribute to a transparent atmosphere.

CYBERSECURITY ERRORS CULPRIT #4:

SIMPLE MISCONFIGURATION

Misconfigurations are happening in even the biggest of companies; these are costly cybersecurity errors exposing organizations to security breaches. The most egregious errors of the past 18 months have surfaced primarily through the exposure of sensitive personal information, business data, credentials, network maps, and more left open to the public inside data stores accessible via cloud-based platforms such as Amazon Web Services S3, Microsoft Azure Cloud, and Google Cloud Platform. Permission errors, API mishaps, and simple misconfigurations have put billion of records at risk to inadvertent access.

Mishaps on AWS S3 and its cloud-based brethren aren't the sole area of concern. Hackers have had a field day with misconfigured MongoDB, CouchDB, and Elasticsearch servers, to the point where attackers were locking down data and extorting ransoms in return for access to these platforms. Ignorance may not be an excuse for cybersecurity errors, but it could be a reason. Organizations may not understand the ramifications of their actions—or inactions—in deploying cloud services and setting up on-premises infrastructures.

How to Break the Cycle. Security must be part of a cloud deployment, and the assumption cannot be made that simply because a service is up and running that it is also secure, and that cloud providers have systems and access locked down. Most providers offer security guidance and configurations that should be followed to reduce exposure and the probability of a breach.

Regular assessments are a must because something as simple as forgetting to set an Amazon S3 storage bin to private could result in weeks of explaining to stakeholders, regulators, and board members. In other words, another instance of a cybersecurity error leading to an otherwise avoidable debacle.

CYBERSECURITY ERRORS CULPRIT #5:

MISSING PATCHES

Vulnerability assessments and penetration tests exist to find gaps in an organization's security posture. The consequences of missing patches, for example, can have critical ramifications for organizations of all sizes. Numerous health care organizations in the U.K., a major telecommunications provider in Spain, and critical infrastructure operators in Europe were among the many that fell hard as the EternalBlue exploit compromised systems globally last year and spread the WannaCry ransomware. The security breach could have been avoided by applying MS17-010, a Microsoft patch available for two months prior to the outbreak. This patch would have closed the hole attacked by EternalBlue. The same is true for the politically charged case of the Panama Papers in 2015, which was brought on partially by an unpatched WordPress bug (the law firm Mossack Fonseca was running a version of WordPress on their main website that was three months outdated).

How to Break the Cycle. Major vendors such as Microsoft, Google, and Apple have automated update mechanisms for security patches, but many organizations opt against this option in order to test patches against their infrastructure. Some updates could break application compatibility and must be tested before being pushed to production environments. These are legitimate reasons for delaying patch deployments, but these decisions must be weighed against the risks posed by the effects of a security breach and attackers seeking to take advantage of the ever-shrinking window of opportunity businesses have between disclosure and the time attacks are in the wild.

CYBERSECURITY ERRORS CULPRIT #6:

INSECURE APPLICATIONS

Applications developed internally or by an independent software vendor will contain bugs, often relatively simple and known vulnerabilities such as SQL injection or cross-site scripting that remain prevalent despite years of advice and remediation to the contrary. Businesses must assess the risk and understand that whether deploying a homegrown web application or a software-as-a-service app, security policies, configurations, and remediations ultimately fall at the feet of the customer.

How to Break the Cycle. To prevent insecure applications from leading to major cybersecurity errors, you will want to ensure their safety by hiring a firm to periodically test your software, or you can rely on an internal team to do the dirty work. It's important that you test how all your software pieces work together. However, ensure that you are vetting any software that you purchase. Ideally, the company that you are relying on values security and has conducted their own research and testing.

AN EXEMPLARY MODEL OF BREACH RESPONSE

CASE STUDY
TIMEHOP

We’ve been talking here about the snowball effect of small security errors leading to large consequences. This concept works in reverse, too: paying attention to the details can get you out of trouble, too.

When social media aggregator Timehop recognized it suffered a breach involving 21 million records, including personal information on 3.8 million Europeans, their response plan was something they had discussed for months. Timehop CEO Matt Raoul and COO Rick Webb had an incident response up and running within three hours.

> *“We knew that we’d got here by moving too fast and leaving open some doors,”*

said Webb, who admits that while they had rolled out multi-factor authentication, they hadn’t done it everywhere - that led directly to the breach. Webb and Raoul decided that they would disclose in a way few companies ever had: total openness. The problem was that GDPR required a disclosure in the first 72 hours, so once again they had to move faster than they’d like.

Timehop decided to put everything on the table: their mistakes, the impact on their customers, and their plans to fix it.

And things went well, considering the scope of the issue. Timehop’s customers were concerned, but understanding.

Then, Timehop found they had more to disclose.

The pair decided to double down.

“We saw that the full disclosure was working,” said Raoul, “and if there was any way to live down the fact that we needed to disclose more it was by saying, ‘Look: we’re doing the right thing, and we made a mistake, but here’s everything we know at this point.’” This time round, in addition to releasing even more detailed timelines of the hack, the full database schemas, complete record counts…everything they could think of, they also invited national journalists into the war room to see what was happening, and how Timehop was responding.

While all this was going on, their team had begun a bottom-up reimagination of the firm’s security, from single-sign on to multifactor across every application, to reconfiguration - a complete re-commitment to getting the small things right. This includes re-architecting some of their environments, adding more automation in deployment, and more vulnerability assessments and penetration testing.

By the third day after the breach, with the investigation and cleanup progressing, the media frenzy died down, and the customers were back in force. It’s not over - the investigation continues, and the jury on European regulators’ response is still out. But Timehop’s commitment to transparency is serving as a model for breach response, and its customers and partners are rewarding them for it.

> *“All of our social media provider partners hung tight with us through the storm,”*

said Webb. “And our customers are telling us the service is more important than ever.

TAKEAWAY
TIMEHOP

The takeaway from Timehop is that when small security errors do lead to the worst-case scenario, a breach, be transparent and show your customers that you are working to quickly fix the issue. The one good thing about falling prey one of these errors is that they are usually are easily fixed. There are several other lessons from Timehop's breach and their response, but ideally you will learn from them as well as the other examples discussed above.

CYBERSECURITY ERRORS GUIDE

CONCLUSION

Where many companies compound these errors is in their response once they learn of the breach. Companies that deny or try to downplay the issue end up parsing language and paying lawyers while alienating their customers. A great example of breach disclosure transparency is Timehop, which chose to quickly and fully disclose not just the breach and the cause, but the entire timeline of what happened, and what it was doing to correct the issues. Its response was a template for companies struggling to understand the new breach disclosure deadlines of GDPR. This kind of response pays dividends over the short term (in customer reaction and trust) and long term (increased brand value).

Don't let cybersecurity errors be the downfall of your organization. Take the time to protect your organization against threats that only require simple mitigations to fade from view.

CYBERSECURITY ERRORS GUIDE

ADDITIONAL
RESOURCES

Bishop Fox Guide: AWS S3 Buckets Security
Avoid Common Mistakes When Deploying Cloud-based Services

ASD guidance on getting the 'basics' right to mitigate targeted attacks:
https://www.asd.gov.au/publications/Mitigation_Strategies_2017.pdf

MEET ALEX DEFREESE

ABOUT THE AUTHOR

Alex DeFreese (OSCP) is a Security Associate at Bishop Fox. In this role, Alex focuses on web application penetration testing, social engineering, and internal network penetration testing. His professional background includes vast experience with performing large-scale penetration tests against enterprise web application. He is especially well-versed in web application testing and has served on multiple client engagements. Prior to joining Bishop Fox, Alex worked as a research engineer at the Georgia Tech Research Institute.

BISHOP FOX.

Bishop Fox provides security consulting services to the Fortune 1000 and high-tech startups.

We find problems before the bad guys do.

Find out more at bishopfox.com.

Keep in touch with the foxes on Twitter @bishopfox and on LinkedIn.

timehop

Timehop reinvents reminiscing

We help people find new ways to connect with each other around the past.

Find out more at timehop.com.

Keep in touch with Timehop on Twitter @timehop and on LinkedIn.