Digital Handout

How good is your safety net?

Crucial facts and figures about cybersecurity in the financial sector

Introduction

With over 27.000 security breaches per year, resulting in a loss of more than 6 billion USD, the financial industry is undoubtedly the most affected sector in the world. In a way, that's no surprise because financial institutions have always been - and will remain - a prime target for cyber-criminals due to what is often referred to as Sutton's rule*.

In this digital handout for the financial industry, together with Erik Ploegmakers - CEO Zerocopter, we share several facts and figures that underline the importance of developing (new) security measures and actively managing cyber risks. And, we also explain what we can do to support financial institutions in the fight against modern-day Willie Suttons.

The Willie Sutton Rule is based on a statement by notorious American bank robber Willie Sutton, who, when asked by a reporter about why he stole from banks, answered: "Because that's where the money is." In other words, his end goal was money, so why waste time looking for it in obscure or questionable places instead of taking the path of least resistance and most success and going straight to the source. | Source: investopedia.com

The most **regulated industry** on **the planet**

The financial industry, which includes various businesses, from banks to insurance agencies, is one of the most heavily regulated industries internationally. To put it in perspective, all European financial institutions must comply with, at the very least, 1.256 regulation articles, each of which can have multiple restrictions. Many of these regulations go towards maintaining the data and financial security of customers and the economy.

Regulations range from local to international, but international laws are often the most impactful. **Here are some of the most influential international data security standards:**

PCI-DSS

Payment Card Industry Data Security Standard

This standard outlines the proper handling of payment card data. Any business, organization, merchant, or payment provider must comply with PCI-DSS standards.

ISO/IEC

International Organization for Standardization/ International Electrotechnical Commission

This standard highlights recommendations for maintaining and improving data security while handling financial information.

CSP

SWIFT Customer Security Programme

Any process that uses SWIFT must comply with this standard, which focuses on handling data, managing security risks, and responding to incidents.

These three regulative standards don't even scratch the surface of what could be considered the bare minimum for most financial institutions. Stacked on top of these are country or region-specific standards and other frameworks that may be service-specific. **Here are a few more recognizable regulations and standards:**

- The Sarbanes Oxley Act (SOX)
- Payment Services Directive (PSD 2)
- General Data Protection Regulation (GDPR)

Pioneers and **Innovators**

With so many regulations, financial institutions are pressed to continually improve security. Being one of the pioneers of the security business, it is no big surprise that finance has one of the most mature industry data and software security frameworks out there. Businesses and institutions alike use arrangements of innovative techniques, many of which were developed at the necessity of the industry.

The techniques that many financial institutions use, such as Static or Dynamic Application Security Testing (SAST, DAST) or Interactive Application Security Testing (IAST), set a standard for industries that require security, but with less urgency. Even Intrusion Detection Systems (IDS), which are a must for modern internet-connected networks, were developed for financial protection purposes. Additionally, having security teams, active security training, and encouraging an agile work style all enhance the industry's security.

The techniques that many financial institutions use set a standard for industries that require security, but with less urgency.

I Why **so much** regulation?

Financial institutions stand in the center of almost every other industry. All industries require money flow, and it happens that the financial sector acts as a middle man for many of those transactions. Inadequate security would leave huge attack surfaces open for criminals to gain access to information. And because the financial industry is at the center of a web of connections, any vulnerabilities can cause ripple effects in almost every other industry.

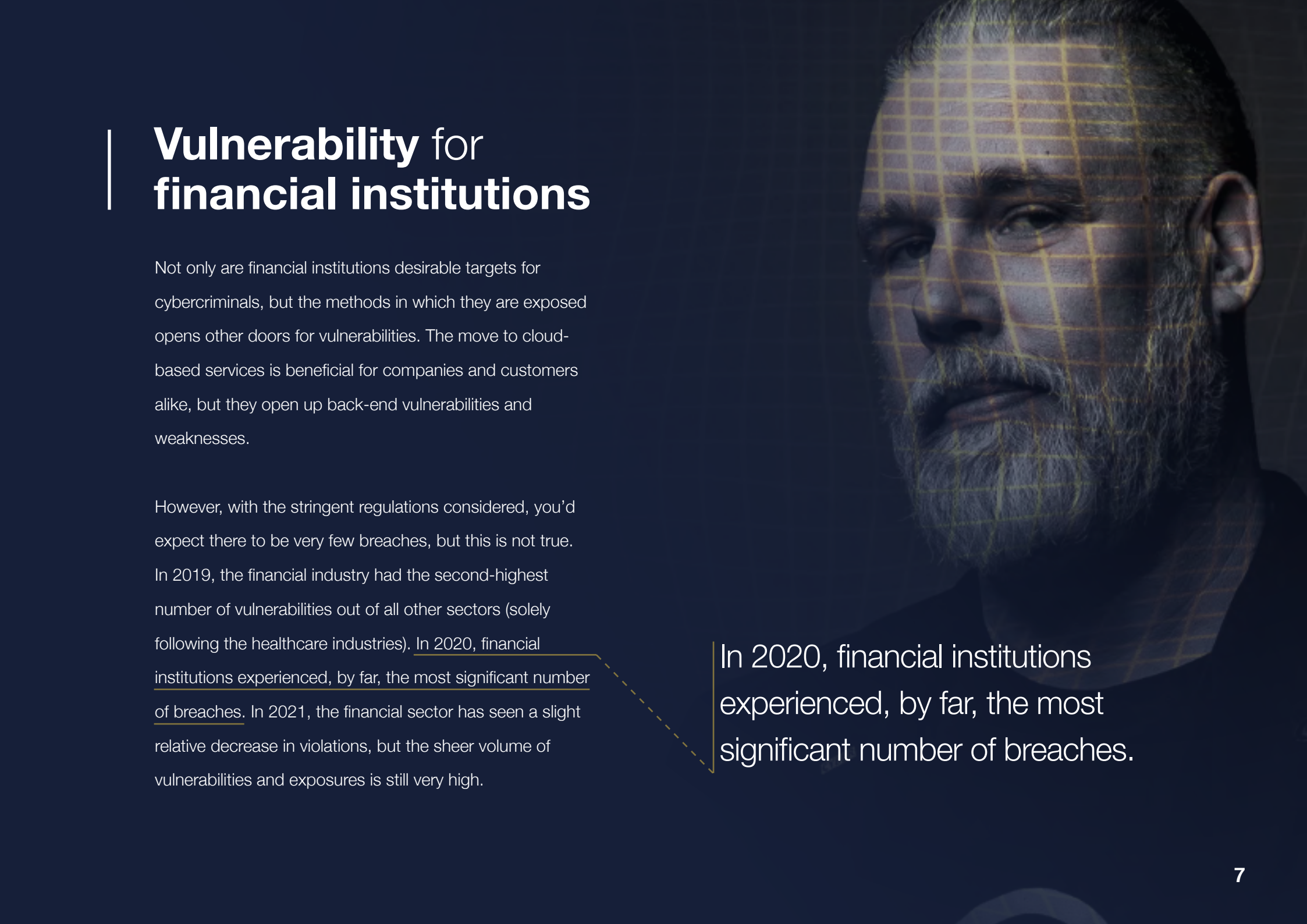
Financial institutions handle very sensitive information that can easily be monetized and used for financial fraud.

In addition to fruitful scope for cybercriminals, financial institutions handle very sensitive information that can easily be monetized and used for financial fraud. This increases the allure for cyber-criminals and thus warrants the significant number of restrictions and regulations.

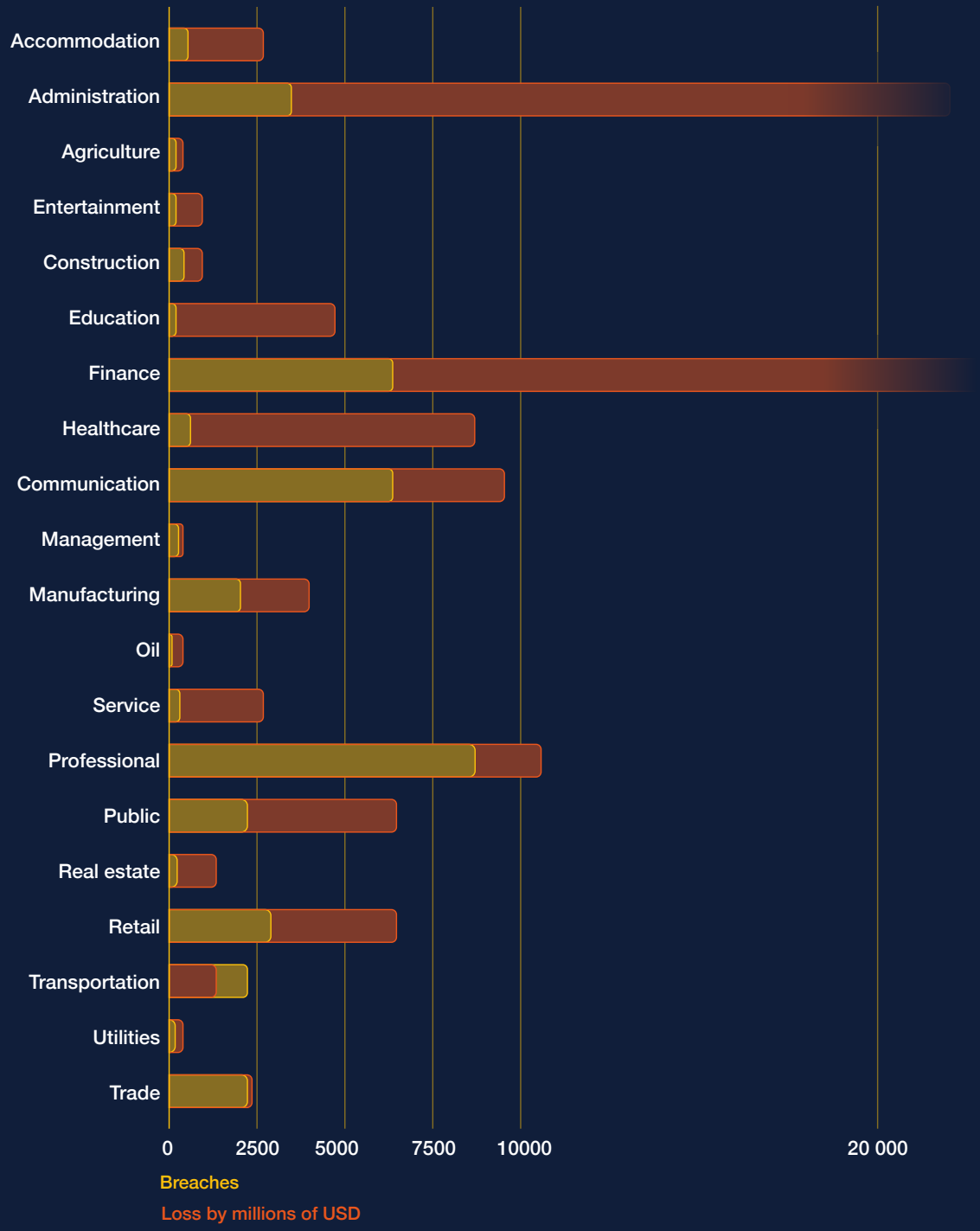
Vulnerability for financial institutions

Not only are financial institutions desirable targets for cybercriminals, but the methods in which they are exposed opens other doors for vulnerabilities. The move to cloud-based services is beneficial for companies and customers alike, but they open up back-end vulnerabilities and weaknesses.

However, with the stringent regulations considered, you'd expect there to be very few breaches, but this is not true. In 2019, the financial industry had the second-highest number of vulnerabilities out of all other sectors (solely following the healthcare industries). In 2020, financial institutions experienced, by far, the most significant number of breaches. In 2021, the financial sector has seen a slight relative decrease in violations, but the sheer volume of vulnerabilities and exposures is still very high.



In 2020, financial institutions experienced, by far, the most significant number of breaches.



Regulations and investment in IT security helps financial institutions avoid massive and catastrophic exposures, and protect a majority of customers in the process. However, many breaches come from tiny and seemingly insignificant exposures, but these make the financial industry one of the most breached. Whether it be an insurance firm or a hedge fund, any significant quantity of vulnerabilities can be expensive.

Number of Breaches by Industry

Loss by Industry

Information from: https://www.bis.org/publ/work865.htm

Zerocopter as a **solution**

Like JPMorgan Chase or Citigroup, massive financial institutions follow every possible restriction, regulation, and framework but still experience the same issue, an enormous number of breaches. This suggests a need for a method past regulations, something additional to provide an extra safety net.

According to Erik Ploegmakers - CEO Zerocopter:

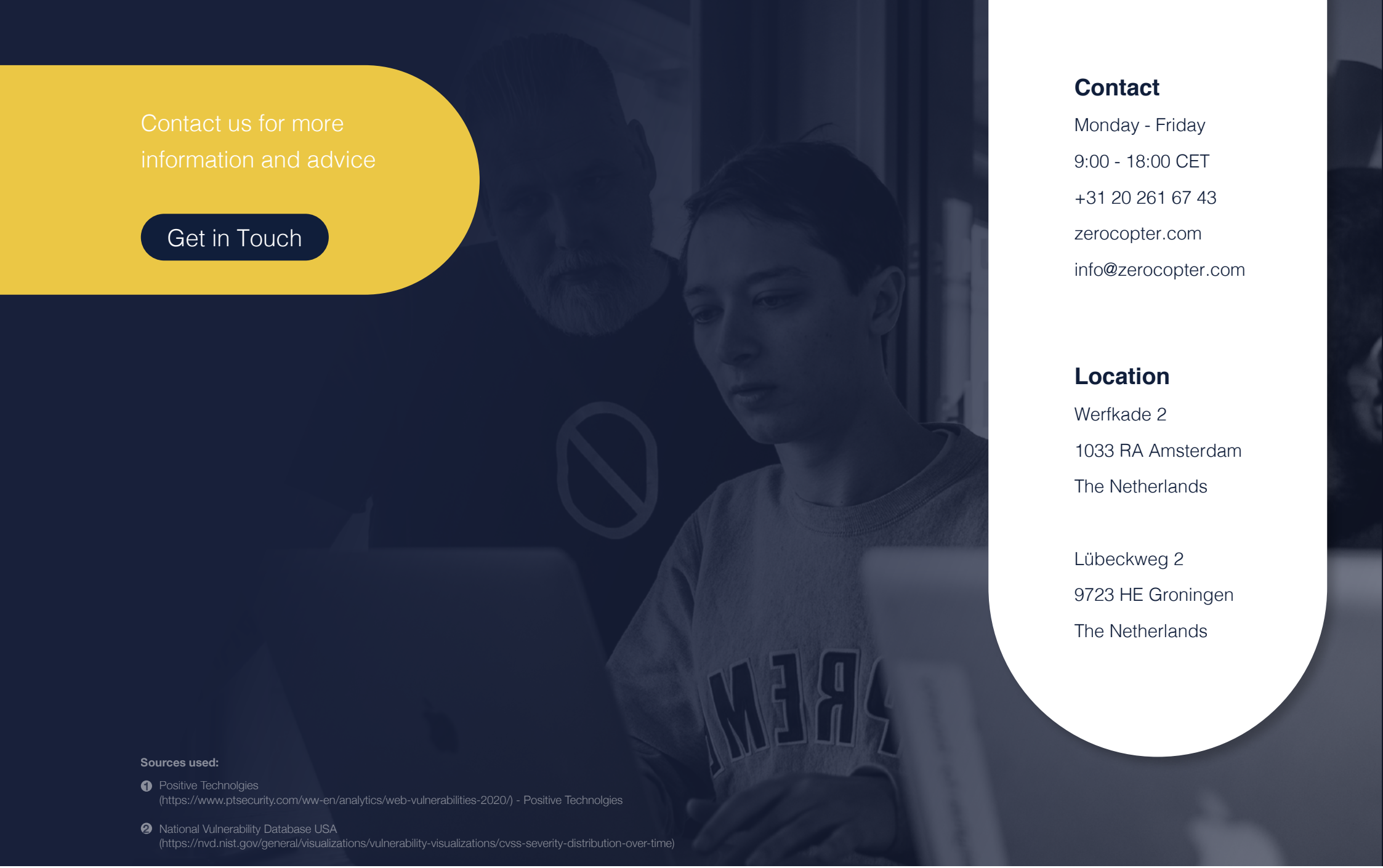
> Although breaches can come from many different places inside and outside of a financial institution, vulnerabilities unidentified within an organization's systems are directly threatening and require immediate action.

This is where Zerocopter can help.
For more information or advice:

Contact us

Zerocopter works with ethical hackers to help identify vulnerabilities within a company's systems, helping to strengthen them against cyber attacks and avoid exposure. The ethical hackers we work with (who we call Researchers) are the best of the best, carefully selected and vetted. This lets Researchers identify and help fix vulnerabilities before criminals have the opportunity to exploit them. Zerocopter works separately from the structured and heavily regulated security systems that are already in place for financial institutions. Our 'unstructured' approach adds a new perspective to security. We act as a safety net, to help catch any vulnerabilities that may slip through the cracks.

In addition, services like Bug Bounty programs can allow for cost flexibility. For example, a company only incurs a cost when a vulnerability is identified in a Bug Bounty program. Additionally, Zerocopter's triage team ensures only valid or unknown vulnerabilities will be accepted. This is a very cost-effective solution for financial institutions that may be unsure whether an additional safety net is worth the cost.



Contact us for more information and advice

Get in Touch

Contact

Monday - Friday

9:00 - 18:00 CET

+31 20 261 67 43

zerocopter.com

info@zerocopter.com

Location

Werfkade 2

1033 RA Amsterdam

The Netherlands

Lübeckweg 2

9723 HE Groningen

The Netherlands

Sources used:

1. Positive Technolgies (https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/) - Positive Technolgies
2. National Vulnerability Database USA (https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time)

zerocopter