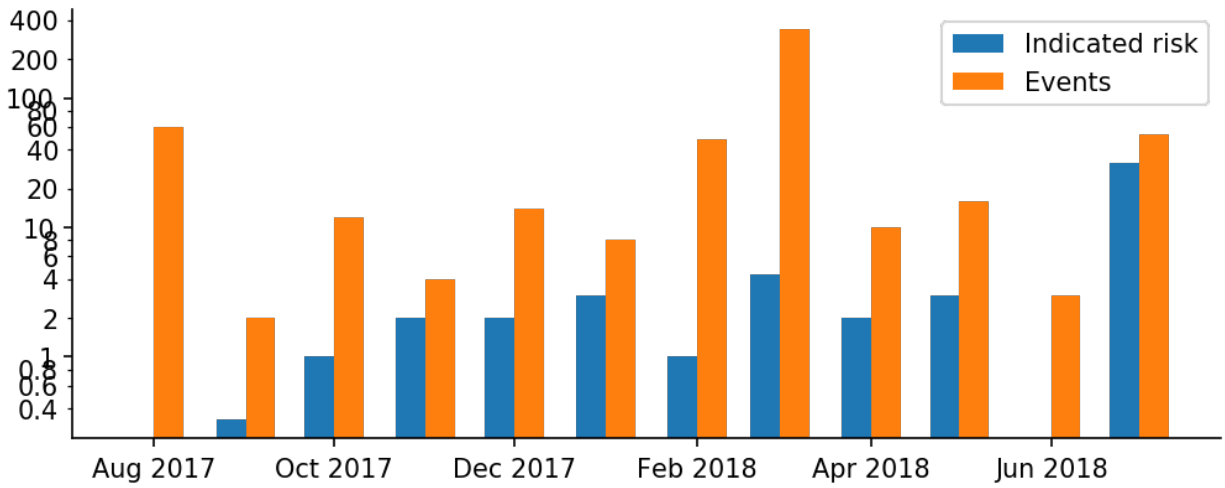
CYBER INTELLIGENCE HOUSE

EXPOSURE REPORT

ACME Corp. - 01.08.2017 - 01.08.2018



Results based on: acme.com

Blue - Indicated risk including:

- **Disclosure of sensitive information:**
  Risk to reputation
- **Exposed credentials:**
  Risk of leaked accounts and password reuse
- **Hacker group targeting:**
  Active efforts aimed at breaching the organisation

Orange - Total number of events including:

- **Disclosure of sensitive information:**
  Risk to reputation
- **Exposed credentials:**
  Risk of leaked accounts and password reuse
- **Hacker group targeting:**
  Active efforts aimed at breaching the organisation
- **External data breach:**
  Risk of data breach in supply chain, partners and 3rd parties
- **Black markets:**
  Risk of IPR violations and loss of revenue
- **Financial information:**
  Financial theft and fraud risks
- **Personally identifiable information:**
  Risk of identity theft and fraud
- **Internal data breach:**
  Indicates a breach in company's own internal systems

HOW TO INTERPRET THE RESULTS

Blue, indicated risk: AI and machine learning algorithms automatically identify and validate about 65% of all events based on the given domain names. Each finding is given a risk weight based on how serious it is.

The greater appearance of orange indicators on page one displays the amount of unidentified events that correlate with the domain names. Finding their significance requires further assessment.

Months that display a high number of activity events and high levels of indicated risk represent the likelihood user accounts were compromised. We recommend conducting an exposure assessment and preparing an incident response.

Months that display a high number of activity events but show no significant levels of indicated risk still imply a necessary and immediate investigation of the activity.

Months with a few activity events require continued monitoring and periodic scans for changes in activity frequency.

ABOUT THIS REPORT

This report can be used to assess an organisation's cyber risk, communicate exposure to stakeholders, meet compliance requirements (for example GDPR, HIPAA, ISAE 3402, SOX, SSAE16 etc..) and manage operational security.

Please note that these results are generated automatically and do not necessarily reflect all possible risks. Providing a full picture of cyber exposure requires a deeper investigation by our analysts, who are available through our more comprehensive Cyber Exposure Assessment.

REPORT PARAMETERS

This report was prepared for ACME Corp. on August 03 2018, showing results for the twelve-month frame of 01.08.2017 to 01.08.2018.

The following parameters were used to generate this report:
Domain names: acme.com
Benchmark industry: Information Technology
Employee count: 12000

CYBER EXPOSURE SCORE

Accumulated risk reflects the sum total of indicated risk (shown in the first graph) over the course of the preceding 12 months. For comparisons of different organisations, we also use a cyber exposure score that is calculated by dividing indicated risk by the number of the organisation's employees.

300+

- **Score:** Extreme Exposure. Typically the organisation has already been breached at this level.
- **Risk:** Compliance, reputation & operative
- **Recommendation:** Conduct immediate asset discovery, vulnerability management and exposure assessment. Start incident reponse procedures and perform follow-ups. Immediately notify data protection and compliance officers and prepare for crisis communications.

200-300

- **Score:** Very High Exposure. Typically the organisation has either been breached, or hacker groups are actively targeting it.
- **Risk:** Compliance, reputation & operative
- **Recommendation:** Conduct immediate asset discovery, vulnerability management and exposure assessment. Immediately notify data protection and compliance officers and prepare for crisis communications.

100-200

- **Score:** High Exposure. Typically the organisation has a large amount of exposed clients, accounts and data at this level.
- **Risk:** Compliance & operative (emerging risks like phishing and targeted attacks)
- **Recommendation:** Conduct immediate asset discovery, vulnerability management and exposure assessment. Notify data protection and compliance officers.

1-100

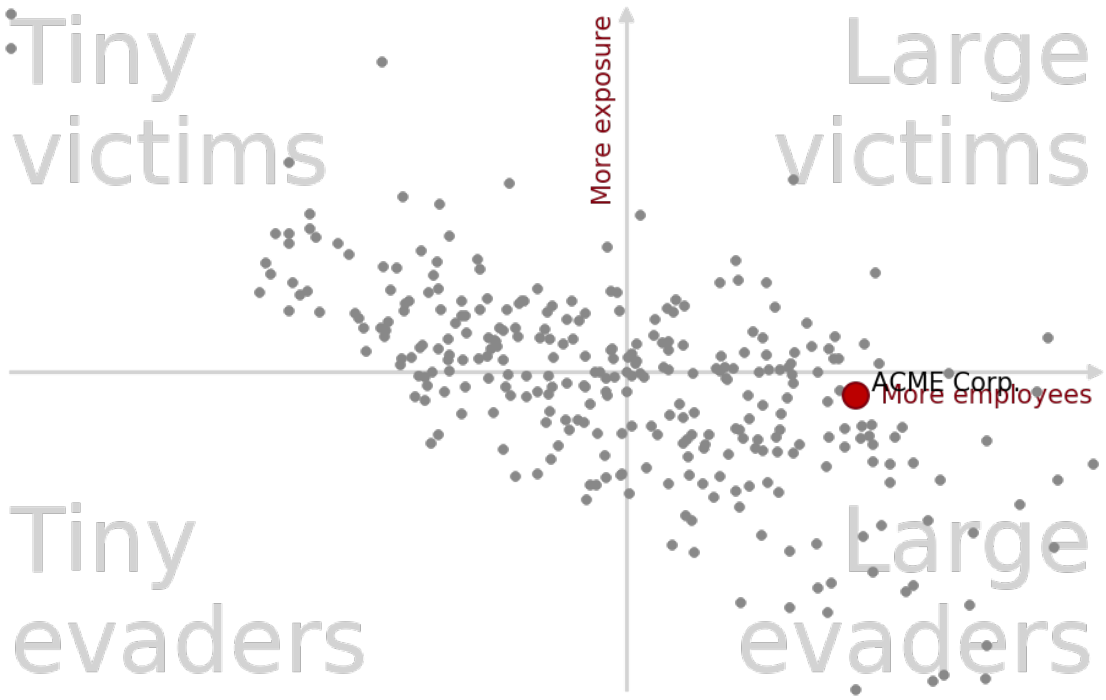
- **Score:** Moderate Exposure. Typically the organisation has a moderate amount of exposed clients, accounts and data at this level.
- **Risk:** Compliance & operative
- **Recommendation:** Conduct exposure assessment to discover the exposure's content and impact. Immediately notify data protection and compliance officers.

1

- **Score:** Low Exposure. Typically the organisation has no automatically identified exposure risks. Some organisations usually discover exposure by using a wider range of search criteria.
- **Risk:** Compliance
- **Recommendation:** Conduct exposure assessment if there are unidentified events matching the given domain names. We advise monitoring the organisation's cyber exposure as well as personal accounts. We do provide a free tool, Hacker for Business, for this purpose.

SCORE WITHIN THE INDUSTRY

The exposure score is displayed against an industry benchmark in the diagram below. Organisation's positioning in the quadrants is a good way to choose an appropriate course of action regarding its exposure.



Tiny Victims, on average, are smaller and more exposed than other companies. Make an assessment of cyber exposure. Use Hacked for business for ongoing protection. Tiny Victims typically lack of security management systems, leadership, processes or culture.

Tiny Evaders are smaller and less exposed. This may be because attackers haven't focused on them, they have good security or perhaps they have just been lucky. Retain low exposure by using Hacked for Business.

Large Victim organisations involve many people and require exposure assessments for better protection. Consider setting up continuous monitoring as large exposure may be a sign of a recurring problem. Large organisations are more vulnerable to phishing and password reuse attacks as these attacks involve employees and other personnel.

Large Evaders are large and less exposed. Consider continuous monitoring to retain low exposure. Due to large number of employees phishing and password reuse attacks may cause cyber exposure to escalate quickly. Defending large organisations is relatively more resource intensive than organisations with less employees.

MANAGING CYBER EXPOSURE

Typically, companies manage cyber exposure by following three steps:

1

PRODUCTS: CYBER EXPOSURE INDEX & CYBER RISK SCORE

Companies and organisations become aware of their cyber exposure. Question often asked: How do we know if we have any exposure?

2

PRODUCT: CYBER EXPOSURE ASSESSMENT

Organisations conduct an assessment to gain in-depth understanding of what information has been exposed and what remediation strategies are available. Questions often asked: What information has been exposed? What can we do to mitigate emerging risks?

3

PRODUCT: CONTINUOUS MONITORING

Organisations develop capability to respond to threats emerging from cyber exposure. Questions often asked: Can we get notifications and alerts in real time when exposure happens?

APPENDIX: HOW CYBER EXPOSURE WORKS

In today's highly digitalised world, data is the primary currency and driver for every business. This means that every business also faces new data-related risks and threats that need to be remediated. By identifying existing threats and making them transparent, the Cyber Exposure Report is the first step in this remediation and mitigation process.

The Kinyako Cyber Exposure Report is based on data collected from publicly available sources in the dark web, the deep web and data breaches. Using this data, we are able to identify signs of sensitive disclosure, exposed credentials and hacker group activity against your organisation.

KEY TERMS USED IN THIS REPORT

SENSITIVE DISCLOSURE

Sensitive information is typically regulated by government laws and organisational policies. Such information should never be stored on your computer's hard drive or on a portable device, and should not be sent via email without proper authorisation. Sensitive information typically includes internal emails and discussions about confidential matters such as business plans, company valuations and trade secrets. The disclosure of sensitive information can result in identity theft, regulatory fines and civil as well as criminal penalties under state and federal statutes.

EXPOSED CREDENTIALS

Exposed credentials include exposed usernames, passwords, tokens or other identifiers that enable access to restricted systems. Exposed credentials are the most common means by which hackers gain access to a system via password reuse attacks. Such information can be exposed through system breaches or information leaks, and can be made available to others either for free or for a price. In many countries, laws require organisations to notify individuals whose credentials have been exposed in a breach.

HACKER GROUP TARGETING

Hacker groups such as Anonymous are loosely associated international networks of activists and hacktivists. They organise attack campaigns that may begin with a published manifesto – a statement explaining the reason for the attack – and are followed by target lists and other communications about performing the attack. When hacker groups target organisations, the result can be an intentional attempt to break into organisation systems or perform distributed-denial-of-service (DDoS) attacks that cause downtime for critical systems. Whether or not such attacks are successful depends on the target organisation's security posture as well as the participating hacktivists' skills and tools.

RISK CLASSIFICATION

Risk is calculated based on the existence of different variables such as identified cleartext passwords, hashed passwords, phishing target lists, hacker group target lists, source code, email messages and internal documents.

The existence of cleartext (human-readable) passwords is considered to be a high risk, as at least 43% of people will reuse their password as is. Hashed passwords are considered to be a medium risk, as they cannot be used directly; however, breaches of hashed passwords have occurred, and – so far – most of the hashes have been cracked after being published.

The existence of individuals on a target list is considered to be a low-risk exposure. While they may indicate an increased risk of phishing attacks, such lists alone do not provide information about the success of those attacks only – about the attempt.

Being a company on a target list is considered to be a medium risk. While this is almost 100% certain to lead to web application attacks and DDoS attacks, the success rates for these attacks are typically not as high as the risk.

Sensitive disclosure concerns the disclosure of internal documents, emails and source code. Such disclosures can result not only from hacking but also from the actions of rogue employees or stakeholders. The risk is medium-level, as the disclosure has already occurred, but the impact varies case by case.

Cyber Intelligence House
www.cyberintelligencehouse.com
www.cyberexposureindex.com
www.hacked-app.com
Paya Lebar Square. Singapore