NormShield

CRITICAL ASSETS & COST-EFFECTIVE RISK DISCOVERY

HACKERS ARE STUDYING YOU RIGHT NOW

Hackers conduct cyber reconnaissance on you:

- Discover your Internet footprint
- Identify weak links

SECURITY ANALYSIS

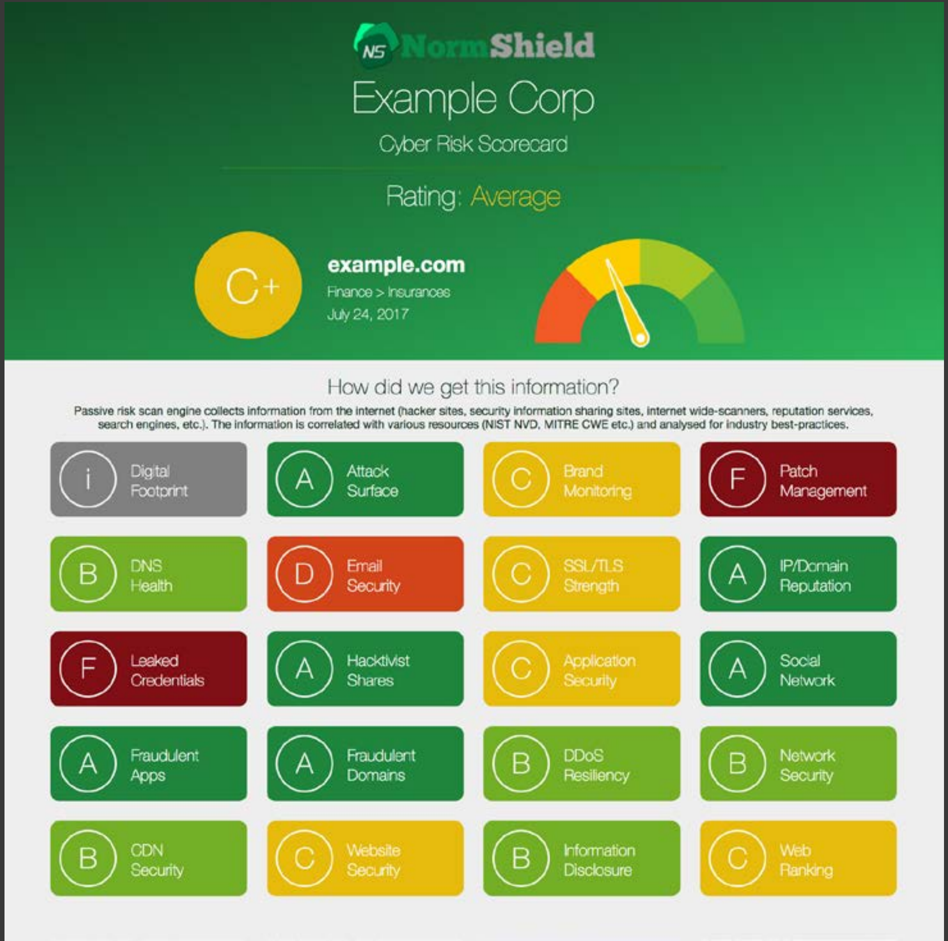
We conducted the same cyber reconnaissance as a hacker --

6 Industries

250 Companies

100,000 Active Assets

THE TOOL WE USED



NormShield

Example Corp

Cyber Risk Scorecard

Rating: Average

C+

example.com

Finance > Insurances

July 24, 2017

How did we get this information?

Passive risk scan engine collects information from the internet (hacker sites, security information sharing sites, internet wide-scanners, reputation services, search engines, etc.). The information is correlated with various resources (NIST NVD, MITRE CWE etc.) and analysed for industry best-practices.

i Digital Footprint	A Attack Surface	C Brand Monitoring	F Patch Management
B DNS Health	D Email Security	C SSL/TLS Strength	A IP/Domain Reputation
F Leaked Credentials	A Hacktivist Shares	C Application Security	A Social Network
A Fraudulent Apps	A Fraudulent Domains	B DDoS Resiliency	B Network Security
B CDN Security	C Website Security	B Information Disclosure	C Web Ranking

DATA COLLECTED IN 5 CATEGORIES

1- Credential Management

2- Vulnerabilities

3- IP/Domain Reputation

Ranked by level of risk

GRADING SCALE

Vigilance required

A It would take world-class, state-sponsored hackers to exploit

B Skills of persistent, experienced hackers are required

Urgent action required

C Average hackers are capable of exploiting

D Beginner hacker practicing their skills

F Script kiddies can hack (i.e. 6th Graders)

OVERALL GRADE

C-

Organizations averaged a C- grade when measured across all categories

Overall, organizations urgently need to protect themselves from novice-to-average hackers

CREDENTIAL MANAGEMENT

WHY IS CREDENTIAL MANAGEMENT SO IMPORTANT?

Hackers use credentials to bypass anti-spam and firewall devices and access users' accounts, then access network and systems

6 out of 10 confirmed data breaches in 2016 leveraged weak, default or stolen passwords. [3]

Nearly 75% of people still use duplicate passwords across multiple systems!

HIGH

PRIORITY.

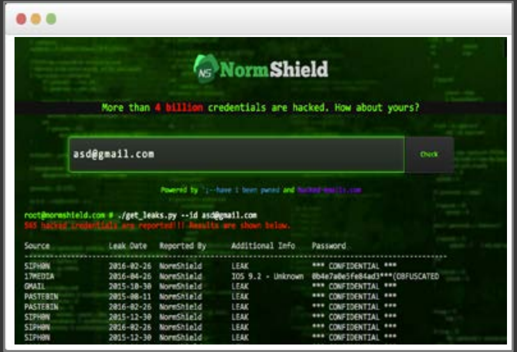
LOW GRADE.

CREDENTIAL MANAGEMENT

D

Urgent! Beginners can use you for target practice.

NormShield found a whopping 95% of respondents had exposed user credentials



NormShield

More than 4 billion credentials are hacked. How about yours?

Powered by ';--have i been pwned and hacked-emails.com

```
root@normshield.com # ./get_leaks.py --id asd@gmail.com
585 hacked credentials are reported!!! Results are shown below.

Source          Leak Date   Reported By    Additional Info    Password
------------------------------------------------------------------------------------
SIPHON          2016-02-26  NormShield     LEAK               *** CONFIDENTIAL ***
17MEDIA         2016-04-26  NormShield     IOS 9.2 - Unknown  0b4e7a0e5fe84ad3***(OBFUSCATED
GMAIL           2015-10-30  NormShield     LEAK               *** CONFIDENTIAL ***
PASTEBIN        2015-08-11  NormShield     LEAK               *** CONFIDENTIAL ***
PASTEBIN        2016-02-26  NormShield     LEAK               *** CONFIDENTIAL ***
SIPHON          2015-12-30  NormShield     LEAK               *** CONFIDENTIAL ***
SIPHON          2016-02-26  NormShield     LEAK               *** CONFIDENTIAL ***
SIPHON          2015-12-30  NormShield     LEAK               *** CONFIDENTIAL ***
```

SIMPLEST THING TO DO

CREDENTIAL MANAGEMENT

Require employees to change passwords at least quarterly with a minimum length of 16 characters

Preferably implement 2FA company-wide

Assume the credentials have leaked and go looking for them regularly

VULNERABILITIES

WHY ARE THEY IMPORTANT?

VULNERABILITIES

- A vulnerability is a hole or a weakness in the application
- It can be a design flaw or a bug
- Attackers exploit to harm the application owner, application users, and other entities that rely on the application

PRIORITY NEED FOR ALL

VULNERABILITIES

C-

Beginner to average hackers are capable of exploiting!

NormShield scanned web applications and network systems against a database of thousands of known vulnerabilities and ranked them in order of severity.

ADDITIONAL FINDINGS

VULNERABILITIES

- 10%+ of respondents had at least one critical issue in web or network assets
- Most had issues due to web servers and applications that were 5+ years old, with unpatched vulnerabilities

Most common & critical vulnerabilities found

1. Misconfiguration
2. Denial of Service (DoS)
3. Information Exposure

SIMPLEST THINGS TO DO

VULNERABILITIES

Monitor/scan public facing systems for known vulnerabilities and apply the patch!

1. Make a list of all security controls and configurations - routers, firewalls, IDSes, AV…
2. Establish the frequency of vulnerability scanning; compare your report against inventory/ control list

IP/DOMAIN REPUTATION

WHY IS IP/ DOMAIN REPUTATION IMPORTANT?

- Employees may download applications that compromise computers and network
- As a result, IP address can become part of a hacker’s network, hosting malware
- This can compromise the company’s brand reputation and lead to a breach

Hackers can leverage IPs for Advanced Persistent Attacks

MANY COMPANIES FAILED

IP/DOMAIN REPUTATION

D+

Urgent! Beginners can use you for target practice.

NormShield checked to see if an organization's IP address has been associated with any blacklists or otherwise involved in malicious activity.

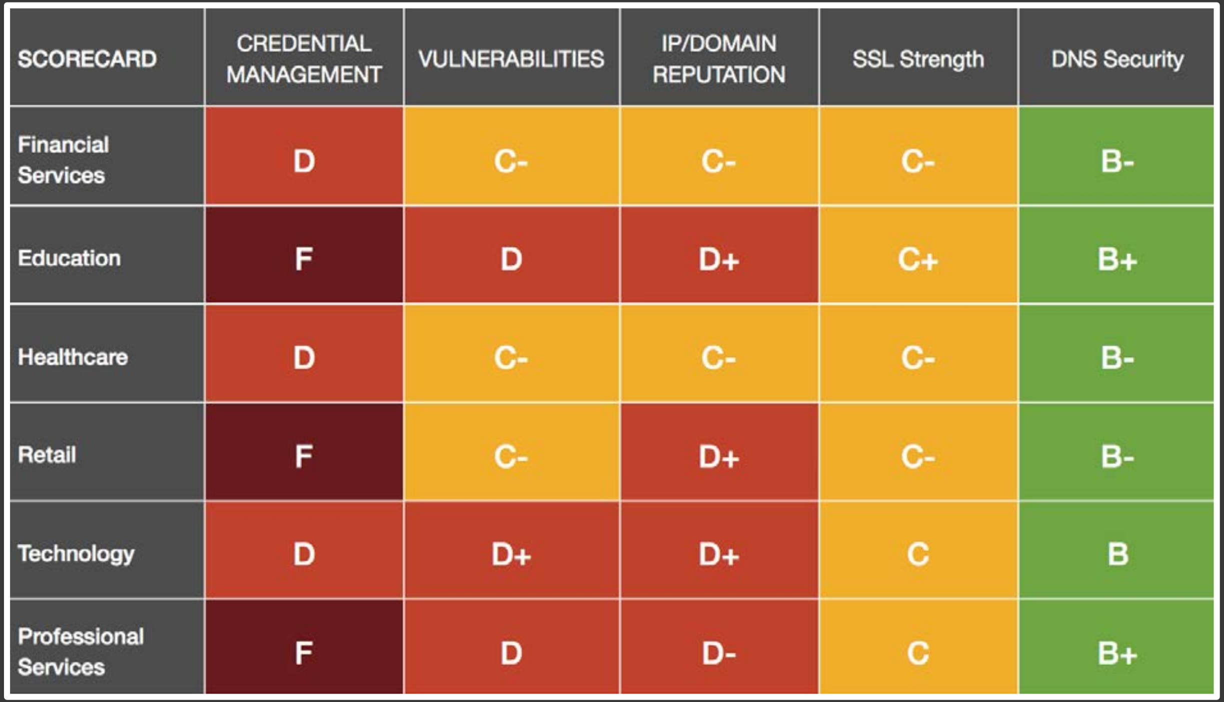
3 of every 5 companies received a D or lower!!

SIMPLEST THINGS TO DO

IP/DOMAIN REPUTATION

1. Monitor the reputation and categorization of your website
2. Ask reputation and content filtering sites to properly categorize your website
3. Block unexpected/malicious traffic on the firewall
4. Change the default resolving IP address of all domains to a whitelisted IP or a loopback IP
5. If possible, avoid using shared servers / IPs with other domains

INDUSTRY REPORT CARDS



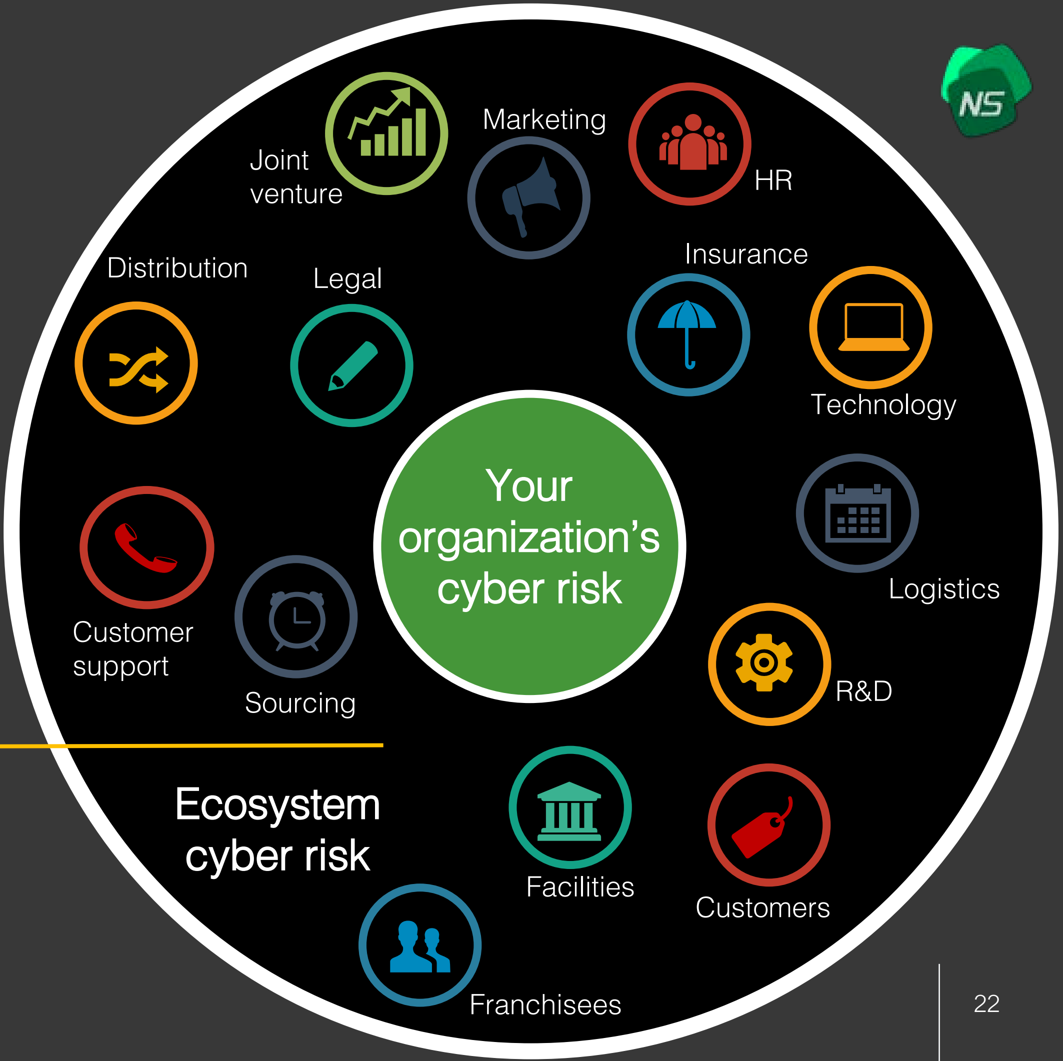
SCORECARD	CREDENTIAL MANAGEMENT	VULNERABILITIES	IP/DOMAIN REPUTATION	SSL Strength	DNS Security
Financial Services	D	C-	C-	C-	B-
Education	F	D	D+	C+	B+
Healthcare	D	C-	C-	C-	B-
Retail	F	C-	D+	C-	B-
Technology	D	D+	D+	C	B
Professional Services	F	D	D-	C	B+

YOUR ECOSYSTEM MULTIPLIES YOUR RISK

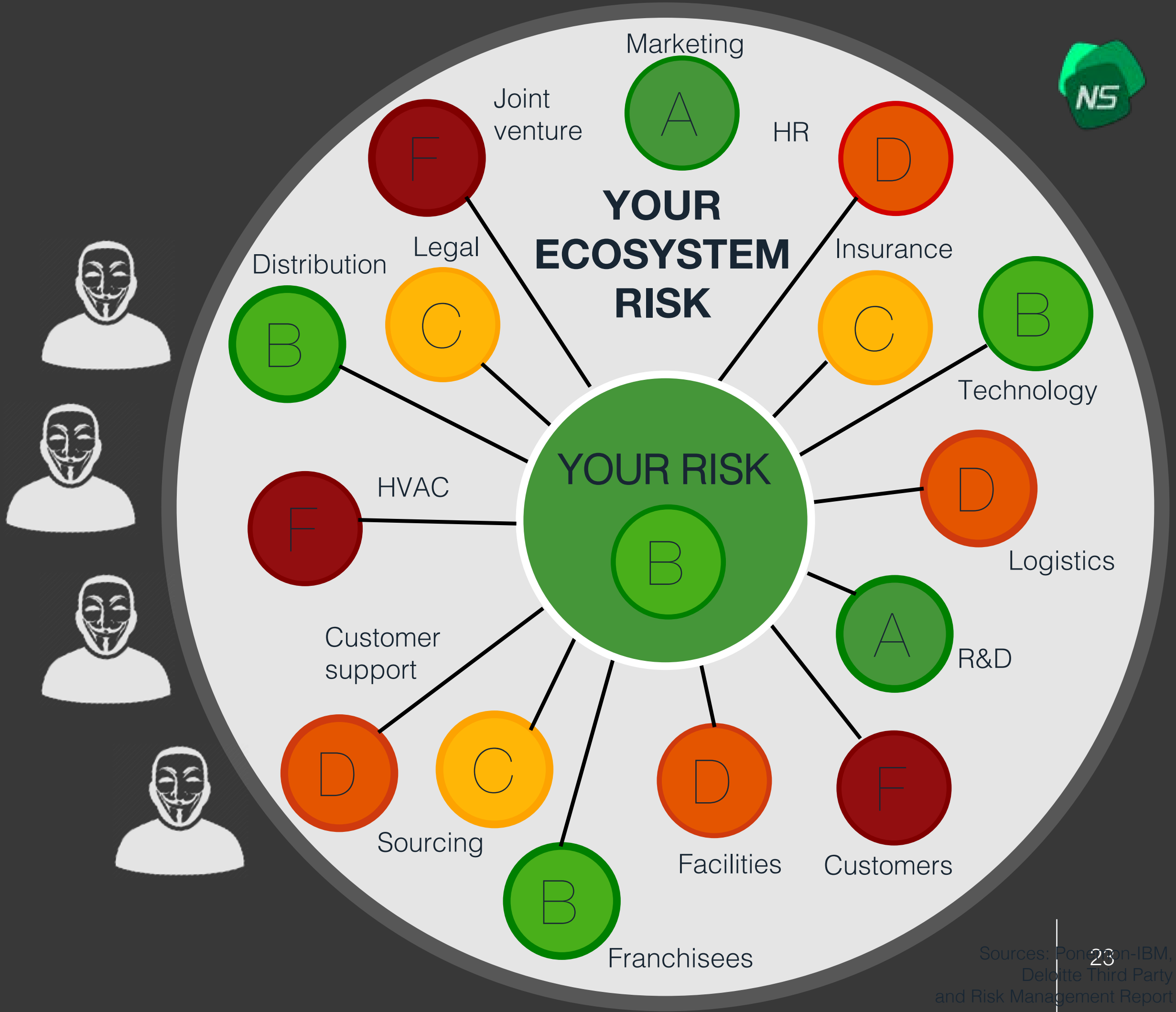
You are only as secure as your weakest partner

63% of breaches originate from hacked 3rd parties

(SOHA Systems)



WHAT IF YOU COULD SEE WHAT HACKERS SEE?



Sources: Ponemon-IBM,
Deloitte Third Party
and Risk Management Report

FIND YOUR RISKIEST ASSETS BEFORE THEY DO

See what hackers see on your own network

Prioritize the highest risks

- Then fix them

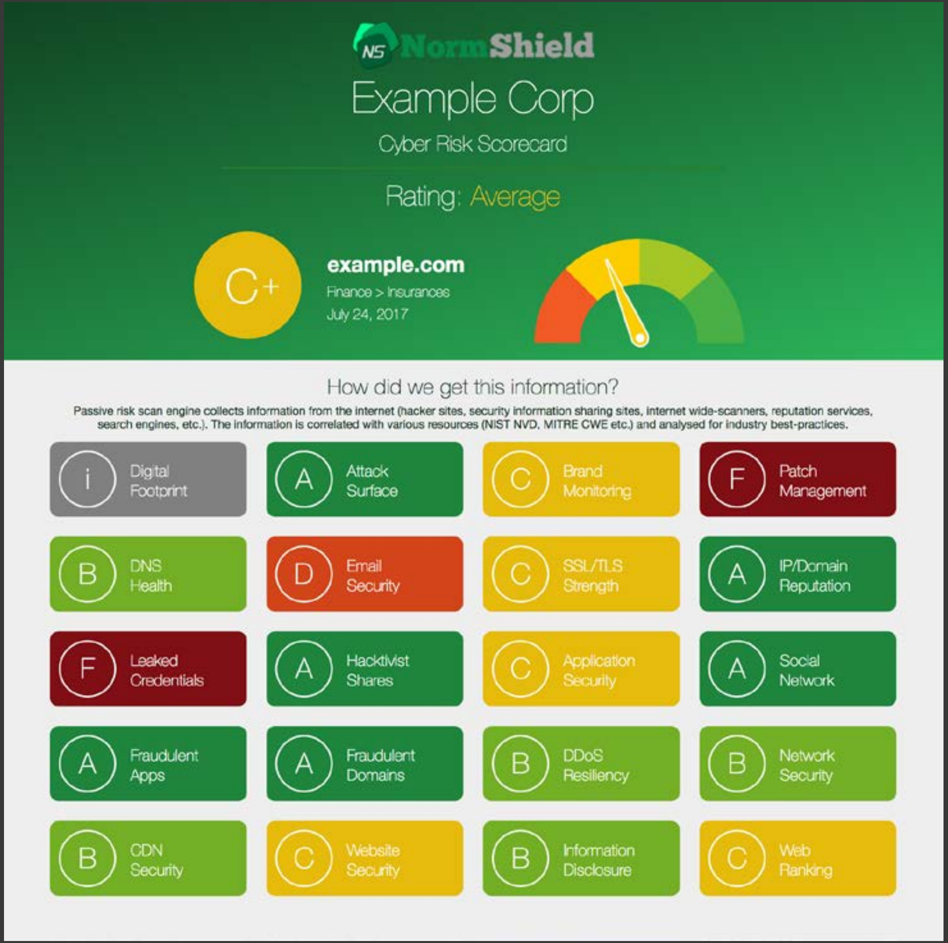
See what hackers see across your ecosystem

- Then set vendor policies

SEE HOW YOU STACK UP

Request your free customized Risk Scorecard

www.normshield.com



NormShield

Example Corp

Cyber Risk Scorecard

Rating: Average

C+

example.com

Finance > Insurances

July 24, 2017

How did we get this information?

Passive risk scan engine collects information from the internet (hacker sites, security information sharing sites, internet wide-scanners, reputation services, search engines, etc.). The information is correlated with various resources (NIST NVD, MITRE CWE etc.) and analysed for industry best-practices.

i Digital Footprint	A Attack Surface	C Brand Monitoring	F Patch Management
B DNS Health	D Email Security	C SSL/TLS Strength	A IP/Domain Reputation
F Leaked Credentials	A Hacktivist Shares	C Application Security	A Social Network
A Fraudulent Apps	A Fraudulent Domains	B DDoS Resiliency	B Network Security
B CDN Security	C Website Security	B Information Disclosure	C Web Ranking

ABOUT NORMSHIELD

The NormShield Cloud platform automates unified vulnerability management, cyber threat intelligence, and risk scoring. CISOs receive letter-grade risk scorecards to make informed decisions. Security teams receive orchestrated, prioritized reporting and automated ticketing for swift action.

NormShield also provides Ecosystem Risk Scorecards to protect you from third party risk.