



# CYBER SECURITY RISK BRIEF 2018





### Rapid Cyber Risk Scorecard

- 60 sec cyber risk assessment
- Non-intrusive scan
- For:
  - SMBs
  - Cyber Insurers
  - Law Firms
  - 3<sup>rd</sup> Party Risk Management



### Comprehensive Cyber Risk Scorecard

- **The most comprehensive & technical** scorecard on the market
- Non-intrusive scan
- For:
  - Medium to Large Enterprises
  - M&A and Due Diligence
  - 3<sup>rd</sup> Party Risk Management
  - Self Risk Assessment



### Threat & Vulnerability Orchestration

- Continuous visibility
- Auto discovery of system changes & anomalies
- Workflow driven orchestration
- For:
  - Large Enterprises
  - Cyber Risk Management

# **NORMSHIELD RISK SURVEY**






Trends and Insights from Cyber Risk  
Scorecard Key Data Points

Includes detailed external security risk  
data from cyber risk scoring for:

- 5127 organizations across multiple industries
- Over 1,000,000 active assets on the Internet, including web and network devices

**DATA  
COLLECTED IN  
5 SECURITY  
CATEGORIES**

Ranked by Level of Risk

-  DNS Security
-  SSL Strength
-  IP Reputation
-  Patch Management
-  Credential Compromise



# 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 five categories
- **Overall, organizations urgently need to protect themselves from novice-to-average hackers**

# DNS SECURITY

B-





## WHAT IS IT?

### DNS SECURITY

When DNS is compromised by a hacker, a user's legitimate application request is redirected to a different network host, possibly with malicious intent

A compromised DNS can damage brand reputation, cause confusion and result in theft





## THE STRONGEST CATEGORY

**DNS SECURITY**

**Companies/Organizations appear  
to have a handle on DNS security.  
Only 20% received a D or lower**

NormShield searched for DNS vulnerabilities and misconfigurations, check both server and protocol implementations

## SIMPLE THINGS TO DO

### DNS SECURITY



1. Use at least 3 DNS servers in different subnetworks
2. Disable recursive DNS response and only respond to authoritative queries
3. Use multiple MX, NS records with different IP addresses
4. Resolve a loopback or a default IP for dormant domains
5. Disable DNS zone transfer from the internet

**SSL  
STRENGTH**

**B-**





## WHAT IS IT?

SSL STRENGTH

- SSL/TSL protocols secure connections between web servers and browsers
- Symmetric & asymmetric cryptographic keys protect credit card transactions, personal information, and other data
- Will soon become mandatory
- Google will label website “unsafe”

HTTP vs HTTPS



## ONE OF THE STRONGEST CATEGORIES

SSL STRENGTH

NormShield investigated the strength of SSL/TSL configurations for 5000+ websites and applications owned by organizations in the study

**More work needed, but lower priority.**

One in five organizations received a D or lower.

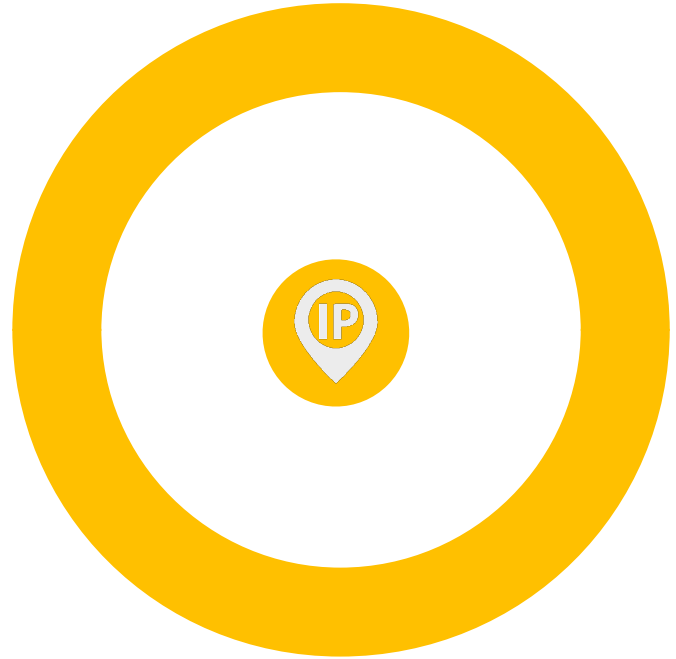
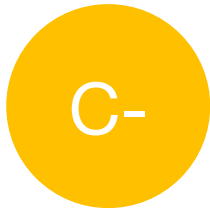
## SIMPLE THINGS TO DO

### SSL STRENGTH



1. Only support strong protocols (TLS protocols - TLS 1.0, TLS 1.1 and TLS 1.2)
2. Use ephemeral key exchanges (Perfect Forward Secrecy - PFS)
3. Only support strong cryptographic ciphers
4. Support TLS-PSK and TLS-SRP for mutual authentication
5. Only support secure renegotiations
6. Disable compression

**IP  
REPUTATION**





## WHAT IS IP REPUTATION?

### IP REPUTATION

Hackers can leverage IP  
addresses for Advanced  
Persistent Attacks

- 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





**MANY  
COMPANIES  
FAILED**

**IP REPUTATION**

NormShield checked if an organization's IP addresses have been associated with any blacklists.

**Warning! Beginners can use for target practice.**

3 of every 5 companies received a C or lower.

## SIMPLE THINGS TO DO

### IP REPUTATION



1. Monitor the cyber reputation
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 (IP addresses used by with other domains)

**PATCH  
MANAGEMENT**





## WHAT ARE THEY?

**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

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

Beginner to average hackers are capable of exploiting!

	<b>Service Version:</b> microsoft iis/7.0 cpe:/a:microsoft:iis:7.0	CVE-2008-0074	7.2
example.com	<b>Description:</b> Unspecified vulnerability in Microsoft Internet Information Services (IIS) 5.0 through 7.0 allows local users to gain privileges via unknown vectors related to file change notifications in the TPRoot, NNTPFileRoot, or WWWRoot folders.		
192.168.100.180	<b>References:</b> <a href="http://www.securityfocus.com/bid/27101">http://www.securityfocus.com/bid/27101</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2008-0074">https://nvd.nist.gov/vuln/detail/CVE-2008-0074</a> <a href="http://www.securitytracker.com/id?1019384">http://www.securitytracker.com/id?1019384</a>		



## ADDITIONAL FINDINGS

### VULNERABILITIES

Most common & critical  
vulnerabilities found

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

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

## SIMPLE THINGS TO DO

### VULNERABILITIES



1. Tracked your assets. Most companies don't know what they own.
2. Identify the criticality of the assets in the organization and each system owner
3. Make a list of all security controls and configurations - routers, firewalls, IDSes, AV...
4. Establish the frequency of vulnerability scanning; compare your report against inventory/control list
5. Classify risks based on likelihood of an attack
6. Monitor/scan public facing systems for known vulnerabilities and patch them.

# CREDENTIAL MANAGEMENT

F







## WHAT IS CREDENTIAL MANAGEMENT?

6 out of 10 confirmed data breaches in 2016 leveraged weak, default or stolen passwords. <sup>3</sup>

- Hackers use credentials to bypass anti-spam and firewall devices and access users' accounts
- Once inside the company network, they can send phishing emails or compromise company systems/data
- Nearly 75% of people still use duplicate passwords across multiple systems!



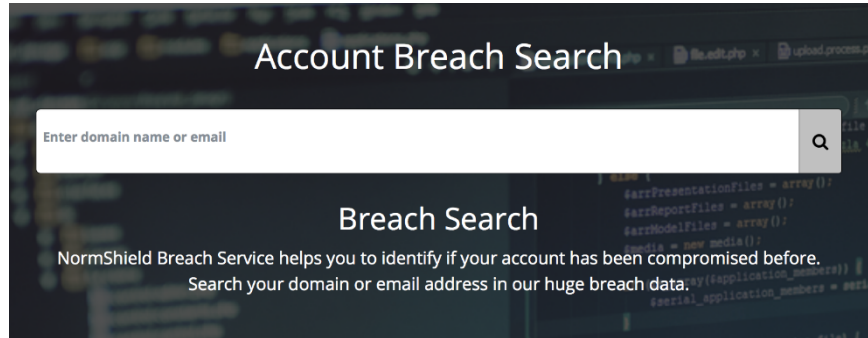
**HIGH  
PRIORITY.  
LOW GRADE.**

**CREDENTIAL  
MANAGEMENT**

NormShield has one of the largest commercial databases of hacked credentials to uncover client exposure.

**Urgent! Beginners can use for target practice.**

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

A screenshot of the NormShield Account Breach Search interface. The page has a dark background with a search bar at the top. The search bar contains the text 'Enter domain name or email' and a magnifying glass icon. Below the search bar, the text 'Breach Search' is displayed. Underneath, a paragraph reads: 'NormShield Breach Service helps you to identify if your account has been compromised before. Search your domain or email address in our huge breach data.' The background of the screenshot shows blurred code from a web browser.

## SIMPLE THINGS TO DO

### CREDENTIAL MANAGEMENT



- Use two factor authentication
- Change passwords at least quarterly
- Educate employees:
  - Do not use company credentials for personal use (social media, online purchasing, etc.)
  - Use different password for business, personal and banking
- Monitor cyber data leaks continuously

# INDUSTRY INSIGHTS

While individual company performance ranged from A to F, no industry group received higher than a C grade when measured across all categories.

# INDUSTRY REPORT CARDS

Categories	Credential Management	Patch Management	IP Reputation	SSL Strength	DNS Security
Financial Services	D	D+	D+	B+	B
Healthcare	F	D-	F	C+	B
Professional Services	F	D-	D	B-	B
Technology	D-	D	D	B-	B+
Education	F	F	F	C+	B-
Retail	F	F	F	B	B-

# INDUSTRY INSIGHTS

Categories	Credential Management	DNS Security	IP Reputation	SSL Strength	Patch Management
Head of Class	<ul style="list-style-type: none"> <li>Financial Services</li> <li>Technology</li> </ul>	<ul style="list-style-type: none"> <li>Financial Services</li> <li>Healthcare</li> <li>Technology</li> <li>Professional Services</li> </ul>	<ul style="list-style-type: none"> <li>Financial Services</li> <li>Professional Services</li> <li>Technology</li> </ul>	<ul style="list-style-type: none"> <li>Financial Services</li> <li>Technology</li> <li>Retail</li> <li>Professional Services</li> </ul>	<ul style="list-style-type: none"> <li>Financial Services</li> <li>Technology</li> </ul>
Back of Class	<ul style="list-style-type: none"> <li>Education</li> <li>Retail</li> <li>Professional Services</li> <li>Healthcare</li> </ul>	<ul style="list-style-type: none"> <li>Education</li> <li>Retail</li> </ul>	<ul style="list-style-type: none"> <li>Education</li> <li>Retail</li> <li>Healthcare</li> </ul>	<ul style="list-style-type: none"> <li>Education</li> <li>Healthcare</li> </ul>	<ul style="list-style-type: none"> <li>Education</li> <li>Retail</li> <li>Professional Services</li> <li>Healthcare</li> </ul>

Hackers are studying  
you right now

Know your cyber  
risk exposure



SEE HOW YOU  
STACK UP



Request a free  
Cyber Risk Scorecard  
at  
[www.normshield.com](http://www.normshield.com)