# DeCort Interactive CyberSecurity Offering

DeCort Interactive, Inc.

Version 2.0

6/6/2017

**DAN DECORT**
E: DAN@DECORTINTERACTIVE.COM
801-934-1527
www.decort.net

## TABLE OF CONTENTS

## OVERVIEW

This informational document will provide an explanation of the cybersecurity offering that is provided with DeCort Interactive and will discuss the importance in taking proper cybersecurity measurements. Security threats continue to rise and it's becoming more important to establish and maintain a healthy online presence.

## THE IMPORTANCE OF HEALTHY ONLINE SECURITY

Many companies do not take into consideration all of the hard and soft costs of a vulnerable website. Online trust with the search engines is a key element for every website. A secure and trusted website will encourage positive search rankings and increase user traffic that will, ideally, lead to revenue conversions through e-commerce and/or form submission channels.

### THE TRUE COST OF A VULNERABLE WEBSITE

The threat of a hack or malicious attack can leave a site vulnerable in the following ways:

a. **RELEASE OF SENSATIVE INFORMATION** – Account information, emails, passwords, etc. are vulnerable to threats of hackers or malicious attacks that leave the company and its clients at risk.
b. **SEARCH RANK CREDIBILITY** – Search rankings may suffer in the event of an attack as a result of the search engine crawling your site and flagging the occurrence. Your search rankings will be penalized, particularly if the malicious content is being placed online through your website. The damage to your search rankings is not instant either. It can take months for the search engine's algorithms to catch up. So, your site's rankings will continue to be penalized long after a solution is implemented.
c. **MALICIOUS CONTENT –** Hackers may illegally seize administrative rights to an account and release malicious/spam content through your site, posing as your company.
d. **COMPANY REPUTATION AND TRUSTWORTHYNESS –** Your company's reputation may be compromised in the event of an attack if your clients' and business partners' information is released or if they, in turn, become the target for malicious/spam content as a result of your site's vulnerabilities.
e. **DISRUPTION/DOWNTIME –** Considerable disruption to your site's operation and/or performance may be affected. Hackers can compromise whole pages, disrupt E-commerce purchases and malicious attacks can potentially take down the entire site.
f. **COST OF DAMAGE CONTROL –** It is imperative that attacks be managed correctly by experienced personnel or your site may continue to be vulnerable. Blocking hackers by eliminating account access, changing passwords and troubleshooting the problem will most likely be required as well as intensive monthly monitoring.
g. **COST OF IMPLEMENTING PROPER MEASUREMENTS –** In addition to the cost of stopping the attack, your company will need to take the necessary measurements to bring its website's security profile up to date. This may include additional developer hours for an audit and implementation of software and hardware updates, changes to the hosting/server

environment, etc. Additional monitoring, as mentioned above, will also be required to reduce and/or eliminate potential future threats.

### COMMON AND TRENDING THREATS

Cyberattacks continue to rise year over year to an estimated 2 trillion globally by 2019 (3) and are a growing threat to businesses across the world. Ransomware, in which hackers take sensitive information from your site and use it as leverage to make demands has increased 300% from 2015 to 2016 with 4,000 daily cases (4). In addition to ransomware, malware, malicious content and hacks also continue to rise.

## KEY ELEMENTS FOR SUCCESS

### CUSTOMIZED SOLUTIONS

Your website is unique and your hosting/server environment should be tailored to your business' needs. There are many options that are scalable to fulfill budget requirements and successfully secure your data. It's also imperative that this solution provided be scalable and able to accommodate your adapting security needs into the future.

### REDUNDANCY

Malware and hacker capabilities continue to grow, adapt and challenge even the best security software. So, it is critical to cultivate a cross-channel approach to minimize vulnerabilities and establish a trusted online presence that search engines will favor.

### REGULAR CARE AND MAINTENANCE

Preventative maintenance is a key factor for the success of your website's cybersecurity. Your site needs constant attention to ensure that software and firmware updates are implemented on a regular basis and to deter and/or prevent malicious attacks. It is also important that your site's security offering be audited and evaluated occasionally to assess its current and future needs.

## COMPONENTS OF SECURITY

### THE HUMAN ELEMENT

It is easy to disregard the importance of human interaction when speaking about technology but it is a critical element. Examples include:

a. **SECURITY PERSONEL**- Data centers that house your site's information need appropriate security personnel staffing.
b. **PASSWORD PROTECTION** – Create good password habits by implementing and periodically updating all passwords.

i. **TWO VERIFICATION AUTHENTICATION PRACTICE** – Multiple verification authentication is a best practice for administrative users on the account. Last Pass https://www.lastpass.com/ is a great resource for this.

c. **ADMINISTRATIVE AUTHORITY** – Layer administrative roles to users ranging from least amount of access; i.e. a contributor, to the most; administrator .

**CONTENT MANAGEMENT SYSTEMS SECURITY**

DeCort's preferred platform for development and design is WordPress because it is the most widely used, open-source content management system (CMS) available on the market today. WordPress takes great care to ensure proper cybersecurity for its users that include, but are not limited to the following (1):

a. **SECURITY PLUGINS AVAILABLE** – For redundant security measurements
**b. FIREWALL**
**c. THREAT SCANNER**
d. **IMMEDIATE AND DELAYED SECURITY PATCHES** – Released upon demand of threat
e. **AUTOMATIC BACKGROUND UPDATES** – Detect threats and eliminate/reduce downtime
f. **FOCUSED RESOURCES** – WordPress targets the top ten security threats per The Open Web Application Security Project (OWASP) 2013 to 10

**SERCURITY WHILE INFORMATION TRAVELS**

a. **SSL CERTIFICATES** – Secure data transfer between web browser and server. Websites with certificates are indicated by an HTTPS notation at the beginning of the URL address.

## THE WAY INFORMATION IS STORED

**HARDWARE BASED SERVER SOLUTIONS**

DeCort Interactive has partnered with Tonaquint Data Center to provide a Tier III Environment for hardware based solutions that include:

a. **PHYSICAL SECURITY ELEMENTS** – Staffed guards, alarms, etc.
b. **REDUNDANT COMPONENTS** – Reduce/eliminate downtime in the event of a catastrophic attack that include, but are not limited to, additional servers distributed in secure locations in the event that Tonaquint's main center is offline.
c. **MULTI-LEVEL CONTROL OF AMBIENT TEMPRATURE** – Keep servers running at maximum efficiency and avoid overheating.
d. **OFFLINE OPERATION** – Expected availability is 99.995% without disruption to performance in the case of an event.
e. **CUSTOMIZED SERVER ENVIROMENTS** may include any one or combination of the following-
    i. **MASTER-MASTER CONFIGURATION** – Data is consistently replicated between servers.

ii. **COMMON FILE STORAGE** – Create consistency of content that is delivered to the user while simplifying data management requirements.
iii. **IDENTICAL REMOTE SERVERS** – Strategically located in secure, offsite locations in the case of a catastrophic event at the primary location.
iv. **KERNALCARE ON ALL SERVERS** – Detects and applies new security patches every 15 minutes.
v. **HACKERTARGET SCANS** – Periodic scans to detect any potential or existing threats.
vi. **MONTHLY UPDATES** – Applied to all outstanding security patches for each server.
vii. **ADDITIONAL UPDATES** – Implemented whenever security bulletins indicate new, vulnerable patches.
viii. **DATABASE NETWORK FILE STORAGES (NFS) AND ELASTIC SEARCH** – Firewalled from public network which restricts access to specific IP ranges.
ix. **ELASTIC CLOUD** – Used to run ElasticSearch to ease load on servers.
x. **LOAD BALANCERS** – Intuitively distributes web requests across servers. In the case of a server failure it will distribute requests to another server to eliminate downtime.
xi. **SFH/SFTP KEY REQUIRED** – All SSH connections require SSH keys to ensure high-level administrative access to directly connect to servers.
xii. **ALL NON-ESSENTIAL SERVICES DISABLED** – Improves efficiency and reduces load on servers.
xiii. **PRIVATE, INTERNAL NETWORK** – Protect and separate all inter-node traffic from the public traffic (DB/ES/NFS).
xiv. **MAXCDN** – Utilized in conjunction with CloudFlare to serve static assets from multiple servers and it specifically hosts .pdf documents where CloudFlare will not.

**CLOUD BASED SERVER SOLUTIONS**

DeCort Interactive's strategic partner for Cloud based server solutions is WPEngine. Cloud hosting environments provide ultimate scalability and multi-level security measurements. WPEngine's security measurements include, but are not limited to:

a. **AUTOMATIC UPDATES** –Minor security patches are automatically updated.
b. **LARGE PATCHES TESTED** – Prior to release all major security patches are tested.
c. **PROPRIETARY INTRUSION PROTECTION** – Allows WPEngine to ward off attacks in real-time.
d. **BLOCK IP ADDRESS** – WPEngine is able to block IP addresses of hackers and/or spammers.
**e. MULTIPLE FIREWALLS**
**f. NETWORK ANALYSIS TOOLS**
**g. PHP TUNING**

**h. DISK WRITE LIMITATIONS AND PROTECTIONS**

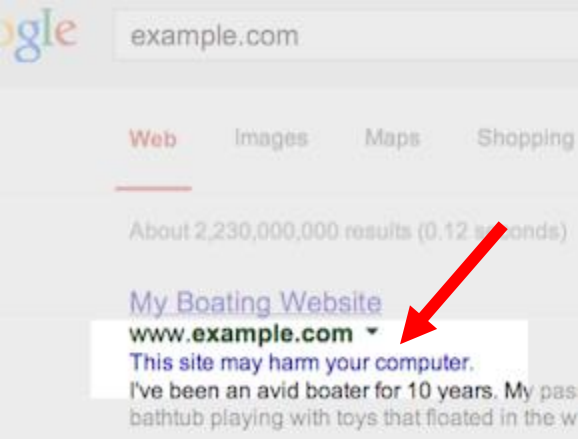
DeCort Interactive also enlists the use of CloudFlare that is a DDoS mitigation service. CloudFlare's security measurements include, but are not limited to:

a. **CACHING AND ROBUST BANDWIDTH** – Absorb attacks without disruption to performance.
b. **SSL CERTIFICATES** – Secure safe transfer of data to server.
c. **DISTRIBUTED NETWORK** – Wards off a targeted, single attack.

## STEPS TO TAKE IN CASE OF AN ATTACK

**EXPEDIENCY**

Immediate care response is critical when identifying and stopping an attack. Attacks, by design, are meant to be difficult to uncover and may be hidden to every day users. However, the attack will not go unnoticed by the search engines as they will periodically crawl websites. If an attack is detected then your site will be deemed untrustworthy. Here is an example of how Google will label your site in the event of a hack.




**IDENTIFY THE PROBLEM**

Get your support team involved immediately and seek professional resources as needed. It may take days or weeks to identify what the issue is and to create a solution to repair and eliminate. Until the problem is fixed, assume the hacker or malware has access to all web content within the site.

**DAMAGE REPAIR**

Once the problem is identified, it is time to eliminate the hack and clean up damage that follows. This will most likely require a coordinated effort from your support team to remove malicious content, eliminate unauthorized users, and update your current security strategy to prevent future attacks. This can be a costly and unexpected project that may negatively affect your business reputation with its clients and vendors since their sites may now be vulnerable as a direct result of an attack on your business' site.

**SUBMIT REPAIR CLAIM TO SEARCH ENGINES**

Your business' search rankings will be negatively affected from a malicious attack, particularly if your site has been labeled by the search engines as untrustworthy. It is possible to reestablish your search rankings by submitting documentation to the search engines that shows the steps your business has taken to resolve and prevent future attacks (2).

**PREVENT FUTURE ATTACKS**

See below for DeCort's best practice recommendations to prevent future attacks.

## BEST PRACTICES

**BUILD YOUR SUPPORT TEAM**

Enlist the help of your website's host, developer and other strategic partners to create an entrusted system with multi-level and cross channel security measurements. Great technology only goes so far and requires trusted personnel to manage.

**CLEAN AND MAINTAIN YOUR SITE**

Regular care and maintenance is critical to maintain long-term cybersecurity. This includes, but is not limited to, software and firmware updates, patches, threat detection, etc.

## SUMMARY

Cybersecurity attacks are becoming increasingly more common and is a major threat to any business with an online presence. These attacks make your website vulnerable by enabling malicious content and/or malware that can compromise sensitive information and embed malicious content and/or spam throughout. It is imperative that your company establish a healthy online presence by creating a support team, regularly maintaining its website and address any threats with the highest amount of expedience.

*Contact DeCort Interactive for more information on how to increase your online cybersecurity @* help@decort.net

## *References*


1. CloudFlare Large-Scale Attacks, https://blog.cloudflare.com/how-cloudflares-architecture-allows-us-to-scale-to-stop-the-largest-attacks/
2. Google https://www.google.com/webmasters/hacked/?utm_source=wnc_633200&utm_medium=gamma&utm_campaign=wnc_633200&utm_content=msg_688800&hl=en
3. Justice.gov https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime
4. Justice.gov https://www.justice.gov/criminal-ccips/file/872771/download
5. Tonaquint Data Center Tier III, https://en.wikipedia.org/wiki/Data_center