ProCircular℠

SECURITY. PRIVACY. TRUST.

Company:

Point of Contact:

Date:

Risk Assessment Summary

The world of information security has become extraordinarily complicated. Every organization, no matter the industry, size, or maturity, will have vulnerabilities. Every day we add new devices, new customer expectations, and expand into new territory for their benefit. Modern organizations are forever bound to computer systems that underpin their operations. Increased utility brings increased complexity. Between various services cracks form, where risks and vulnerabilities are exposed.

In summary, **REDACTED**'s vulnerability assessment reinforced the quality of the work done by the information technology group. Our initial expectation was that the organization would have significant issues given the size of the organization's IT infrastructure and the scope inherent in that of an **REDACTED INDUSTRY.**

You'll see in the following pages that while there are a few issues that require attention, the overall health of the border and online presence of the organization appears to be healthy. It is worth noting that this is a free assessment, and a more in-depth and manual assessment and penetration test that allows for attack traffic is advisable. We also note that there is a *significantly* larger network that was not in scope comprised of a number of domains.

Additionally, in conversations with the principals of the organization we see opportunities to establish a more formal governance approach, particularly given the compliance and uptime requirements of an **REDACTED**. Many of the technical steps may have been taken, but policy, procedure and employee awareness are all areas where **REDACTED** could improve its security posture.

Lastly, people are the cornerstone of all security programs. We recommend improving your employee participation in protecting the organization with Employee Awareness Training.

The basic results of the initial vulnerability assessment.

Risk Assessment Scope

Assessed Entity: [redacted]
Address:
Telephone:
Contact:
Type of Assessment:
Risk Assessment Scope: The scope of this assessment encompasses the potential risk and vulnerabilities to the confidentiality, availability, and integrity of identified systems and data that the company creates, receives, stores, or transmits.
Domains
Domains [redacted]

ProCircular's Approach

ProCircular's approach and tools are customized for each assessment based on the scope and agreed upon business objectives. In order to keep our work with you safe, affordable, and as discreet as possible, we've put together a unique, blended method using both vulnerability assessments and penetration testing. It includes the following:

- Online Presence – We analyzed your website and sites that we could associate with your organization. We scanned those systems using modern tools for thousands of vulnerabilities and weaknesses.
- Network Security - We applied similar tools to your border security to deduce what you look like to the Internet. This often uncovers Internet-facing devices, out-of-date hardware and software, and frequently a few other surprises.
- Principal's PII Search – We did a search for Personally Identifiable Information (PII) linked to selected leaders of the organization. These results will be presented privately.

What this assessment did NOT include?

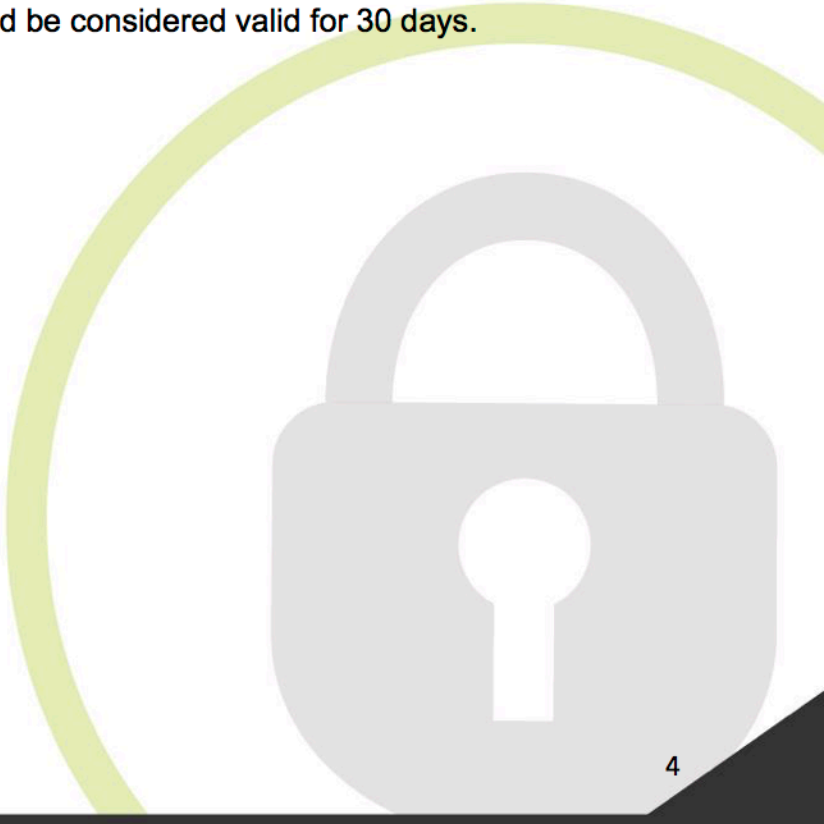
While our assessment is more detailed than what most security firms provide, there are limitations. Here's what isn't included:

- **We're didn't break into your network.** This analysis was strictly limited to outside testing and we didn't make *any* attempt to breach the border of your organization.
- **We didn't try to break anything.** There were no "Denial of Service" attacks or malicious code exploits run against your systems. And while there was always an outside chance of a brief interruption, we've designed these tests to minimize the chances of any potential downtime.
- **We don't point fingers.** Security is *everyone's* responsibility, and we're not the organization that's going to make light of any gaps that stem from any one individual. Each finding is anonymized to protect your employees from being singled out.

Our *free* initial vulnerability assessment doesn't include everything. Your information systems are likely complex and unique to your business. We offer a number of in-depth testing options and other special services as a follow-up to the initial lite vulnerability assessment. While it's a wide look at your firm, it didn't include everything on your network or out on the Internet.

Timing is everything

Many of the findings you'll read about in this document are time sensitive, as are the results. Vulnerabilities and security in general are a moving target, and there's a shelf life to any assessment. If you wait too long, there will likely be a new set of issues added to this stack, and another assessment may be required in order to address the new set of issues. Therefore, the results of this assessment should be considered valid for 30 days.



Risk Framework – Our Approach

ProCircular uses a commonly accepted risk analysis framework based on a number of standards, in this case the NIST 800-30rev1. The definitions of the most critical terms are important for the purposes of this analysis.

Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Most information system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally), or have been applied, but retain some weakness.

Threat

A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat events are caused by threat sources.

Threat Source

A threat source is characterized as:

- The intent and method targeted at the exploitation of a vulnerability
- A situation and method that may accidentally exploit a vulnerability.

In general, types of threat sources include:

- Hostile cyber or physical attacks;
- Human errors of omission or commission;
- Structural failures of organization-controlled resources (e.g., hardware, software, environmental controls);
- Natural and man-made disasters, accidents, and failures beyond the control of the organization.

QUICK DEFINITIONS

Vulnerability:
A security vulnerability is a weakness in a system that could allow an attacker to compromise the integrity, availability, or confidentiality.

Threat:
Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Threat Source:
Those who wish a compromise to occur.

Likelihood

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

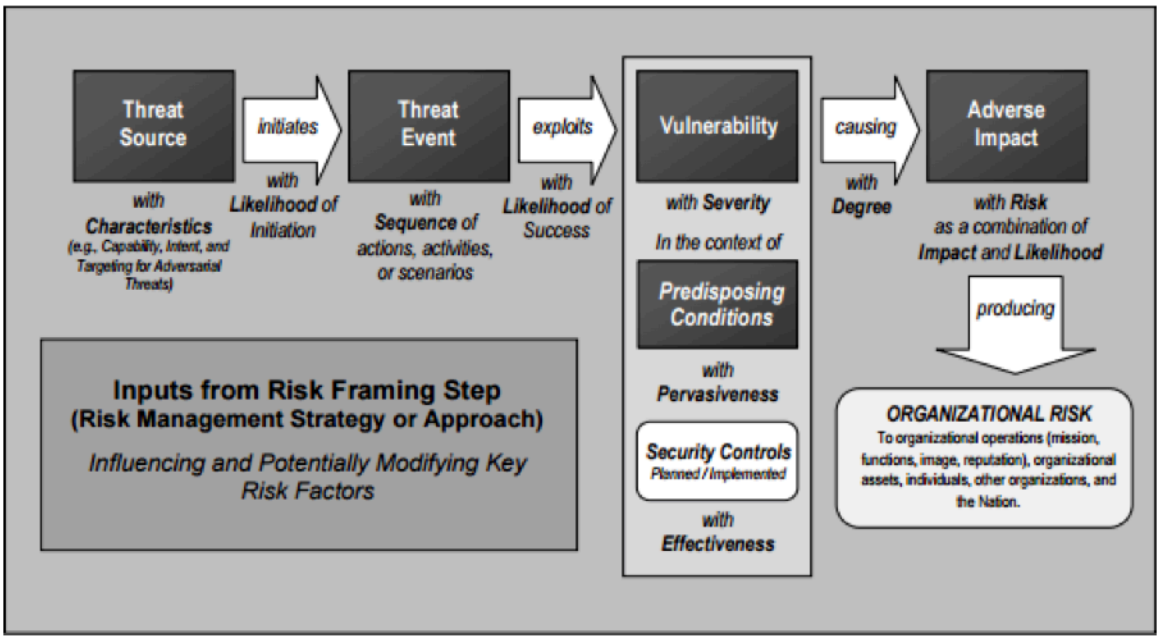
Likelihood Score	Range
1 = Unforeseeable	Not foreseeable at the current time
2 = Foreseeable	Foreseeable in the next year
3 = Low	Foreseeable in the next 6 months
4 = Medium	Likely in the next month
5 = High	Highly likely at the current time

Impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability

Impact Score	Customer or Employee Impact
1 = Negligible	No harm to customers or employees
2 = Low	Customers or employees would be inconvenienced, but would be protected from harm
3 = Medium	Some customers or employees may be harmed financially or reputation, but recoverable
4 = High	Many customers or employees may be harmed financially or reputation and would result in company loss
5 = Critical	Most customers or employees will be harmed financially or reputation and will most likely result in company loss

Risk



Source – NIST 800-30rev1 2012

As noted above, **risk** is a function of the *likelihood* of a threat event's occurrence and potential adverse *impact* should the event occur. This definition accommodates many types of adverse impacts:

- **Tier 1:** Damage to image or reputation of the organization or financial loss.
- **Tier 2**: Inability to successfully execute a specific mission/business process
- **Tier 3:** The resources expended in responding to an information system incident.

It also accommodates relationships among impacts (e.g., loss of current or future mission/business effectiveness due to the loss of data confidentiality; loss of confidence in critical information due to loss of data or system integrity; or unavailability or degradation of information or information systems). This broad definition also allows risk to be represented as a single value in which different types of impacts are assessed separately.

For purposes of this assessment, risk is grouped according to the types of adverse impacts and the time frames in which those impacts are likely to be experienced.

Risk Aggregation – Measuring the Risk

We combine Impact and Likelihood into the following matrix in order to establish **Risk.** ProCircular uses risk aggregation to roll up several discrete or lower-level risks into a more general or higher-level risk.

Risk aggregation, conducted primarily at Tiers 1 and 2 and occasionally at Tier 3, assesses the overall risk to organizational operations, assets, and individuals given the set of discrete risks. In general, for discrete risks (e.g., the risk associated with a single information system supporting a well-defined mission/business process), the worst-case impact establishes an upper bound for the overall risk to organizational operations, assets, and individuals.

Risk Score: **Combined effect of Likelihood and Impact**			Impact				
			1	2	3	4	5
			Negligible	Low	Medium	High	Critical
Likelihood	5	High	5	10	15	20	25
	4	Medium	4	8	12	16	20
	3	Low	3	6	9	12	15
	2	Foreseeable	2	4	6	8	10
	1	Unforeseeable	1	2	3	4	5

One **example** of the use of this matrix would be a lack of endpoint (PC) protection. If workstations are left open to malware, the likelihood that this vulnerability could be compromised is High. The impact could range from Medium to Critical depending upon the form of malware in question, but in general we would rate that as a High impact issue given recent examples of exploits. (e.g. Target, Home Depot, etc.)

Findings

As mentioned earlier, **REDACTED**'s external vulnerabilities earned a relatively low risk number. The upper bound of this matrix is 25 – Critical Impact and a High Likelihood.

Risk Category Identified	Likelihood	Impact	Risk Score	Recommendation	Service Offering
Employee PII Identified	2 (Foreseeable)	3 (Medium)	6	Reset all passwords, training and awareness	vCISO & Employee Awareness Training
Vulnerabilities	2 (Foreseeable)	4 (High)	8	Patch servers, improve patching process	Full Network Assessment
No SSL/TLS	3 (Low)	4 (High)	12	Upgrade servers, implement standard server hardening	Full Network Assessment

Employee PII Identified:

Employee Personal Identifiable Information (PII) was identified on 10 individuals with **REDACTED** email addresses. 3 of those 10 employees have passwords publicly available on the internet as part of a recent breach (Adobe and LinkedIn breaches).

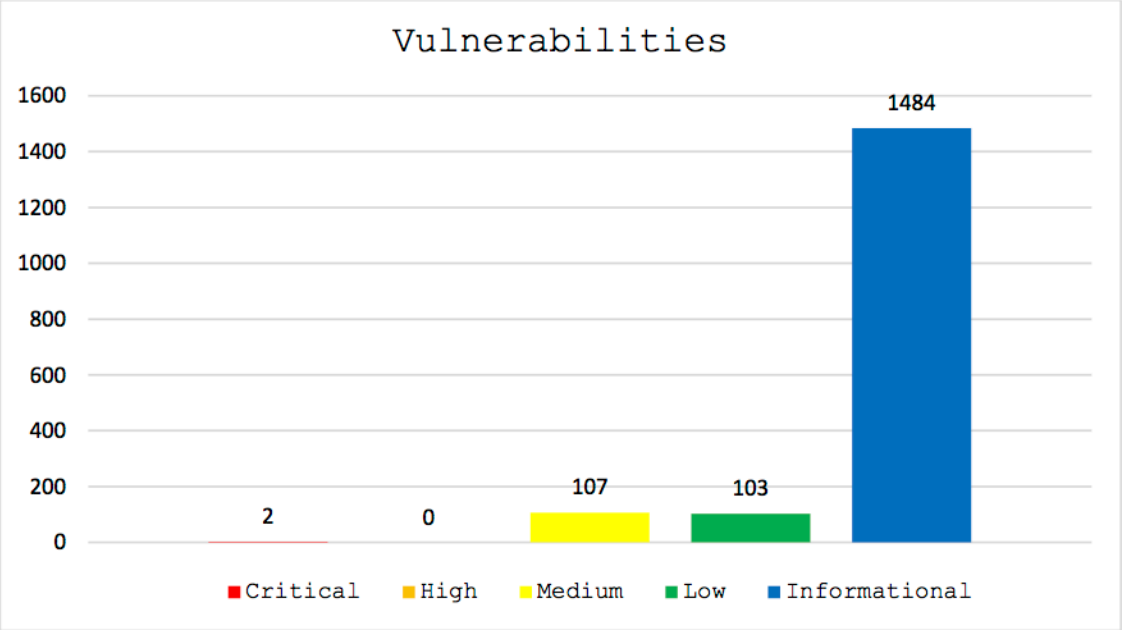
The Risk of Employee PII being Identified is a Foreseeable in the next year likelihood with a potential impact of some customers or employees being harmed financially or reputation, but recoverable. The result is an overall LOW risk score (6).

Vulnerabilities and lack of SSL/TLS:

212 vulnerabilities and missing SSL/TLS was identified on multiple **REDACTED** domains, sub-domains, and IP addresses. Most of the vulnerabilities were Medium or Low but they are still exploitable. The lack of basic security encryption of data in motion via SSL or TLS needs to be addressed.

The Risk of vulnerabilities and missing SSL/TLS has a Foreseeable or Low likelihood in the next 6 months to a year with a potential impact to many customers or employees resulting in financial or reputation harm that would result in company loss. The result is an overall MEDIUM risk score (8-12).

The bar graph below displays the distribution of Vulnerabilities found by ProCircular, during this vulnerability scan. Please refer to section 3.2 in the appendix for more details.



Next Step	Rationale
Virtual CISO (vCISO)	• Security Strategy • Demonstration of Security to 3rd Parties • Incident/Breach Response
Full Vulnerability Assessment & Penetration Test	• Full Scan of network • Determine *real* risk to hackers • Complete remediation roadmap
Employee Awareness Training	• Enlist employees in your defense • Protection from latest threats • Establish importance of security

Recommendations: Virtual CISO (vCISO)

(Entry Level Option - [redacted] thereafter)

Let us show you the way and improve your security together.

For organizations with significant data security needs but limited staff capacity, a dedicated ProCircular employee will perform the function of your Chief Information Security Officer (CISO). This Virtual CISO service is ideal for organizations looking to tap a seasoned expert without the full expense of bringing one on staff.

Drawing on their previous experience as in-house CISOs, ProCircular vCISOs define data security strategies and manage implementation with your organization's executives, IT, and additional security stakeholders.

Many companies have responded by adding a Chief Information Security Officer (CISO) to lead their security program. Not every organization can afford one of these highly trained—and highly-compensated—professionals.

ProCircular can bring that level of reassurance and credibility to your roster. Functioning as a Virtual CISO, we can be the frontline authority for your security program and privacy/compliance regimen. We'll work with your team to manage and improve on your existing security program or help to build a new one from the ground up. This will include:

- Steering committee leadership or participation,
- Compliance management
- Policy analysis and development
- Incident Response Planning
- Establish a Training and security awareness program
- Enable internal audits
- Access to a wide array of other services at a reduced cost

Your customers get the reassurance and confidence they need, your vendors are able to check their boxes, and you receive the benefits of a diverse team of security specialists at a fraction of the cost.

Recommendations: Full Vulnerability Assessment & Pen Test

(One-time investment of [redacted], subsequent yearly tests depending on maturity)

Learn what would happen if you were hacked BEFORE you're hacked.

Our Free Vulnerability Assessment is just a taste of our capabilities. When you need to delve deeper, ProCircular collaborates with your IT department to begin a Full Security Evaluation, unleashing our "Red Team" to conduct a comprehensive vulnerability assessment and in-depth penetration test.

Examining your organization's internal network, social media presence, cloud activity, wireless access, endpoint gaps, and even physical security, we leave no stone unturned, looking in places you often don't, or haven't ever thought of. We take on the role of a hacker in search of your valuable information and provide you with all of the results.

- **Online Presence** – We'll take a close look at your website and sites that we can associate with your organization. We scan those systems using modern tools for thousands of vulnerabilities and weaknesses. Once identified, we will attack those systems using state of the art tools and collect whatever information available.
- **Network Security** - We'll apply similar tools to your border security to deduce what you look like to the Internet. This often uncovers Internet-facing devices, out-of-date hardware and software, and frequently a few other surprises.
- **Cloud Security** – Given a list of your most common cloud services providers, we will run a series of active tests against the providers to try and identify gaps.
- **Social Presence** – This step analyzes a few of the places where your organization is visible online and what sort of data can be easily assembled from what you've posted.
- **Social Engineering** – Anonymous calls to your organization, we'll see what sort of information we garner, and testing using modern few phishing attempts. This provides insight into your organization's overall awareness without pointing fingers at individuals.

We combine the results of all of these tests and present you with a comprehensive report of our findings and recommendations to your staff on appropriate next steps. Yes, it can be daunting (for executives and IT staff alike) to be under such scrutiny, but the results are often rather eye opening. Hackers can do it every day *without* your knowledge. Just remember, we're on *your* side; we're not there to cry wolf, point fingers, or justify our services.

Recommendations: Security Awareness Training

(One-time investment of [redacted] programs available quarterly or yearly)

Creating employees capable of protecting their workplace

Security is only as strong as the people who ensure it. Once our systems are in place, we'll help you build a healthy, living culture of security awareness that will endure long after our work is finished. We'll engage your employees with training sessions and materials, get them involved and aware of their role in the security program, teach them how to work smartly and securely, and create a team mentality with your organization's security at the center.

Your employees will not only learn what not to do, they'll act as your greatest line of defense and secure the place that they love to work for. Our on-site Security Awareness Training will prepare your employees for all of the following:

- Introduction to Computer Security
- Beware of Scams – Phishing
- Avoiding Social Engineering – empowered response
- Protect Information when using the Internet and email
- Passwords 101
- Mobile Devices and Wireless
- Working with Different Types of Data
- Protecting PII and Restricted Data
- How to Report a Security Incident

Very soon we will also offer a Continued Employee Awareness program that keeps everyone up to date once you've made the initial investment in their knowledge. A combination of online training and videos with the latest "things to look out for" will ensure that the employees continue to be on the lookout for threats and bad actors.

ProCircular℠

SECURITY. PRIVACY. TRUST.

ProCircular, Inc. is an Information Security and Privacy firm offering a full-service, client-based approach to help customers protect their data and that of their customers. Specializing in corporate security strategy, infrastructure and cloud-based engineering, and security program design, our experts partner with yours to create durable long-term solutions that fit your business.

Powered by industry experts, driven by client success.

Please allow us to earn your **Trust** and business:
solutions@procircular.com

595 Ashley Court
Suite #5
North Liberty, IA 52317

(319) 359-2632

Find us on: