Colorado Cybersecurity Center Scorecard

Purpose of the Scorecard

The purpose of this scorecard is to gain an understanding of where your company is from on outsider's perspective, This Scorecard is to seek information, accountability, Recognition, feedback and improvement. We are committed to providing you with the best information possible, so we welcome your comments. Please fill out this questionnaire to help NCC-CCC better. Thank you.

How many devices on your network are fully patched and up to date?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

Vulnerability scans and vulnerability management is one of the 20 CIS Controls that can reduce the risk of vulnerability exploits.

Can employees introduce malware or other cyber risks with their own devices to your network?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

A network intrusion detection systems are an important part of your organization's security.

How many times have bad actors attempted to gain unauthorized access?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

Has a bad actor breached your information assets or networks before?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

How long do security threats go unnoticed?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

MTTD measures how long it takes your team to become aware of indicators of compromise and other security threats.

What is the mean response time for your team to respond to a cyber-attack once they are aware of it?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

A great measure of the quality of your incident response plan implementation.

How long does it take to close identified attack vectors?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

How aware is your administration of your companies Scorecard?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

Security ratings are often the easiest way to communicate metrics to non-technical colleagues through an easy-to-understand score. Security ratings can feed into your cybersecurity risk assessment process and help inform which information security metrics need attention.

What is your vendor security rating?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

The threat landscape for your organization extends beyond your borders and your security performance metrics must do the same. By continuously monitoring vendor risks, you can greatly reduce your third-party and fourth-party risk.

How long does it take your team to implement security patches or mitigate high risk CVE-listed vulnerabilities?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

Cybercriminals often use threat intelligence tools and exploit the lag between patch releases and implementation. A great example of this is the widespread success of WannaCry, a ransomware computer worm. While WannaCry exploited a zero-day vulnerability called EternalBlue, it was quickly patched but many organizations fell victim anyway due to poor patching cadence.

How many users have administrative privileges?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

Access control and the principle of least privilege are simple, cost effective methods of reducing privilege escalation attacks.

How does your organization's cybersecurity scorecard compare to your peers in your industry?

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

This information is easily digestible, visually appealing and highly compelling which makes it a top choice for board presentations. This Scorecard allows you to easily benchmark your security performance against industry peers over the last twelve months.

Rate your vendors incident response time.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Disappointing Exceptional

A security incident is not just a successful cyber-attack; intrusion attempts to vendors can signify your organization as a potential target. The longer it takes vendors to respond to incidents, the higher the chance you will suffer from a third-party data breach. In fact, some of the biggest data breaches are result of poor vendor management.