CYBERSECURITY SCORECARD

Michael Gilliam | Manager of Cybersecurity Services
mgilliam@ddaftech.com | 859.425.7794

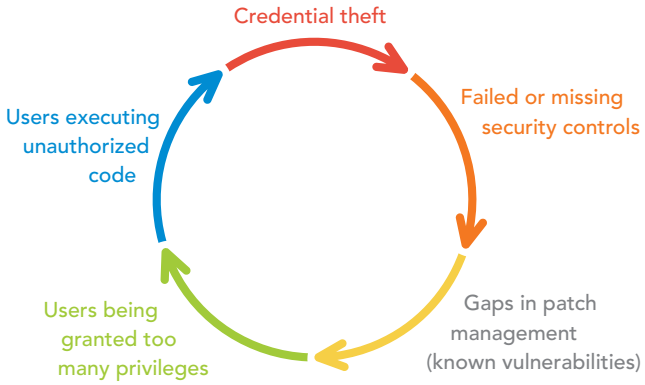
DEANDORTON
TECHNOLOGY

CYBERSECURITY SCORECARD

In 2018, more than 43% of malware related breaches occurred in small businesses—but most small businesses don't have the budget for the expertise or assessments that will help them improve their security posture. Because of this, small businesses often become an easy target for opportunistic malware threats distributed by organized cybercrime syndicates. Small businesses are left with many questions:

- How much security is enough?
- How do we know what we are doing is enough?
- What does a security program look like?
- How do we make security measurable, actionable, and attainable?

Dean Dorton has created a proprietary process that helps measure key elements of your security program, and focuses on providing actionable remediations to improve your organization's security posture. The process in non-invasive, highly automated, and can generate updated results of your entire security posture within hours. These elements can be measured on a monthly, quarterly, or annual basis to help your organization track your progress on your security journey. Our focus when building this process was to ensure organizations are covering all of the main aspects commonly used in breaches, without overly complex security frameworks. Most security breaches are a direct result of a few, common issues, as illustrated in the circular chart to the right.



In light of this, Dean Dorton has created an assessment (Cybersecurity Scorecard) that groups these issues into four core security domains that are measured:

EXTERNAL SECURITY

- Attack surface review
- Vulnerabilities
- Remote authentication
- IP reputation

ENDPOINT SECURITY

- Malware protection
- Endpoint hardening
- Endpoint compliance
- Vulnerabilities

COMMON CONTROLS

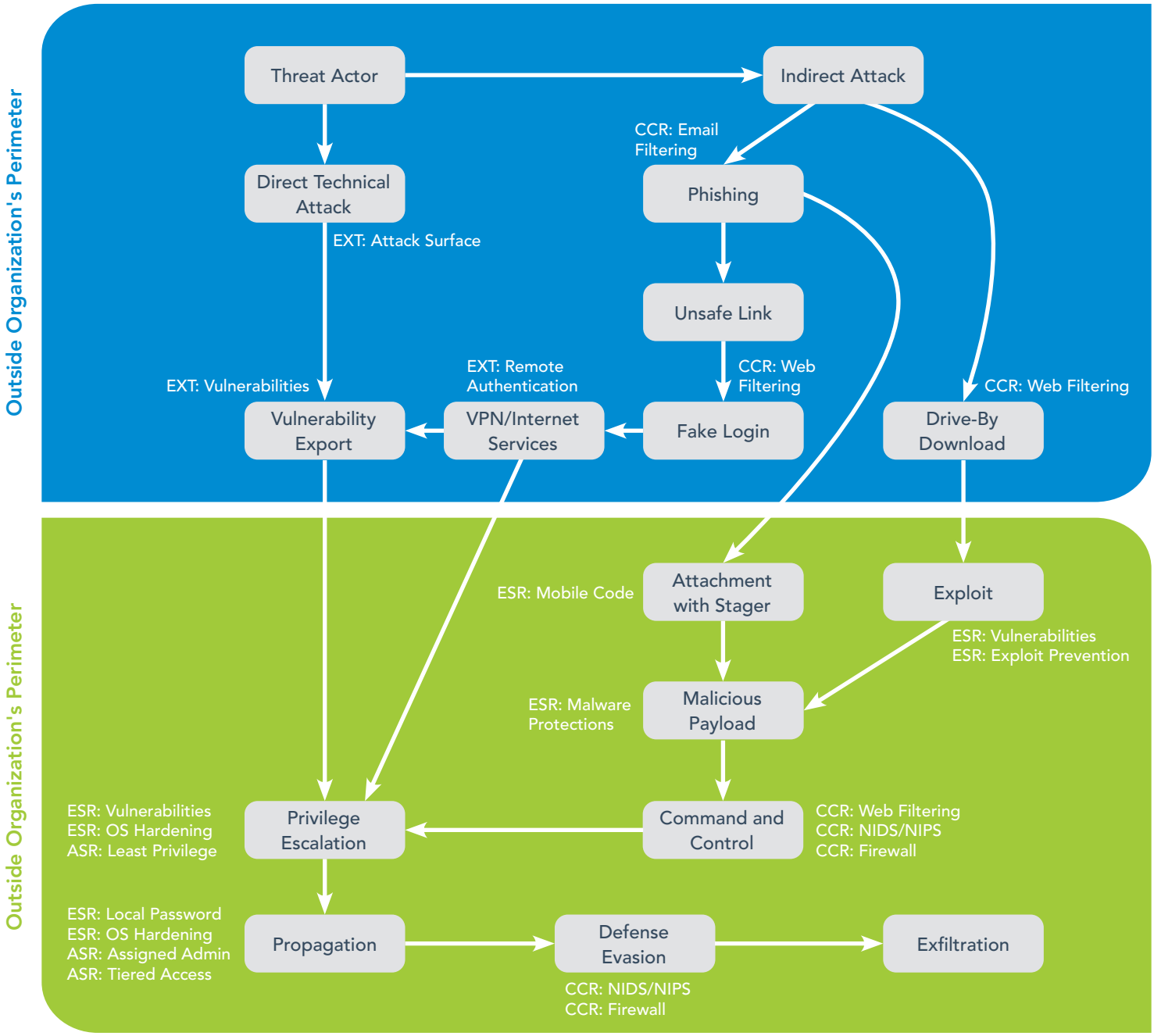
- Security monitoring
- Firewall
- Email filtering
- Network monitoring
- Web filtering

ACCOUNT SECURITY

- Password policy
- Privileges of logged-on users
- Administrative rights
- Tiered access

WHY USE OUR SCORECARD?

Dean Dorton carefully chose the core domains and sub-areas for review based upon knowledge of how the most common attacks occur. By taking a methodical approach to these cyber kill chains, we aligned the security issues or controls that directly correlate to the tools, tactics, and procedures used. By rating the effectiveness of an organizations approach to each area, we can provide a holistic view of the risks posed.



EXT – External Security
ESR – Endpoint Security Review
ASR – Account Security Review
CCR – Common Controls Review

WHY USE OUR SCORECARD?

Measuring issues individually is not sufficient; it is the process in which Dean Dorton is able to combine observed security issues ***down to the host level*** which makes this offering special and allows organizations to act quickly to pinpoint where the greatest risk lies.

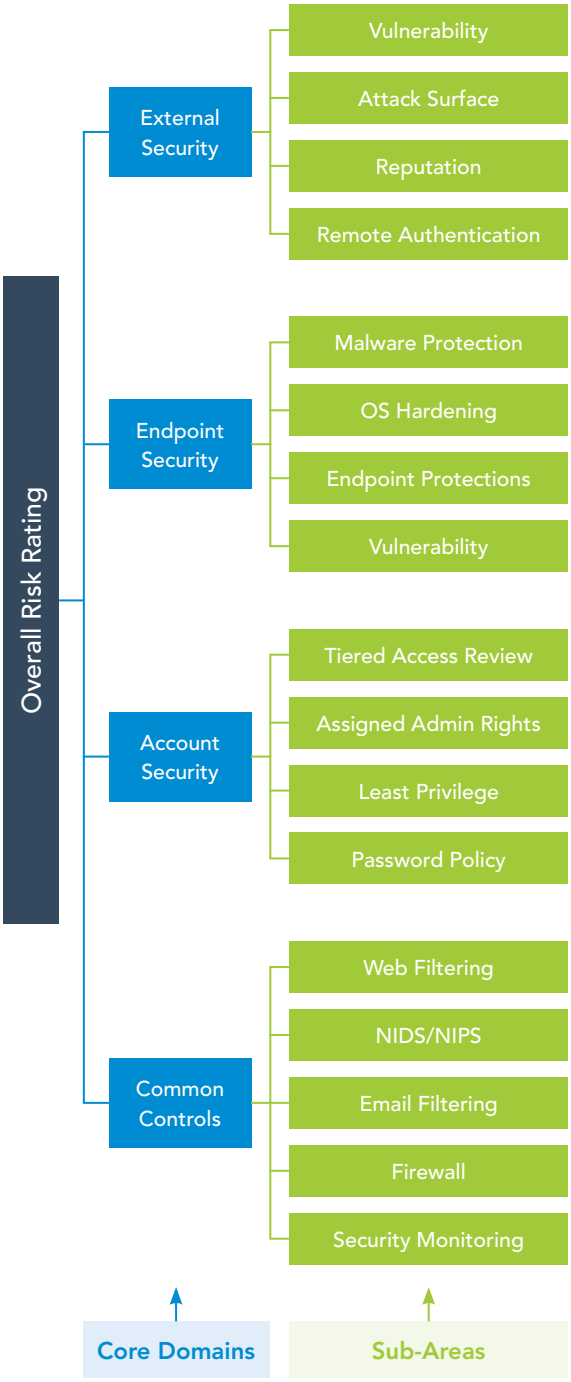
Take, for example, a system with **outdated Antivirus Definitions**. This system does not inherently pose a tremendous amount of risk. However, combined with **multiple critical vulnerabilities** and a **user who logs in with local administrator rights**, you have a situation in which that particular asset poses a large risk for the organization.

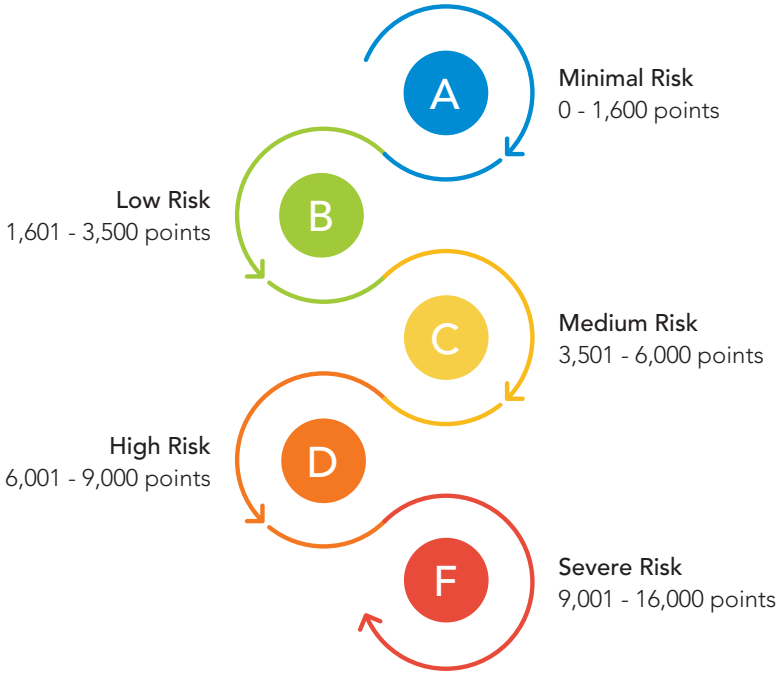
Furthermore, consider that, while you have one risky asset, your organization may have layered common controls (such as email and web filters) configured in such a way that your overall risk is lower (though you may have some individual assets that need attention).

Unlike other offerings, the Dean Dorton Cybersecurity Scorecard uses details gathered from hosts inside and outside your network through our data collection process while on site. To provide additional overall context to these details, we perform interviews with your system administrators to determine the level of common (or shared) controls used to provide layered defenses. These common controls, combined with account, endpoint, and external information, provide a high level view your organization's risks to the most common threat actor tactics, and how your efforts can be applied most efficiently to reduce your risk. This information is crucial to understanding your organization's posture and providing details on how to improve your status.

SCORING THE SECURITY DOMAINS

We use a color-coded risk point scale for scoring provided on the core security domains and for the overall risk score: the more points scored on an area, the higher your risk level. Your organization is given a cyber risk grade, determined by how well the organization performs on the security domain.





Sub-Areas

Each core domain is made up of several sub-areas that are analyzed and scored. Sub-Areas are graded on a point scale depending on the number of areas in the domain, but usually of 4,000 points per area.

Core Domains

The sum of the score for each of the sub-areas in a core security domain is used to calculate the Risk Score for the entire domain.

Overall Risk Grade

The scores of the four core security domains are averaged and used to generate an overall Grade/Risk Level for the organization. The finalized metrics will be presented in the form of a PDF report as well as executive summary PowerPoint presentation.