DEANDORTON

Cybersecurity Scorecard



Small businesses are being targeted nearly four times more than large organizations according to the 2025 Verizon Data Breach Investigations Report. Rapid 7 research indicates that companies ranging from 11 to 1,000 employees make up 64% of ransomware incidents–where the median ransomware payment alone (not counting downtime, reputation damage, and recovery services) averages between $170,000 and $200,000. 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?

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

PASSWORD SECURITY

- Group Policy Preferences
- Domain Password Audit
- Local User Password Management
- Password Policy
- Saved Password Exposure
- Password Manager Deployment
- Passwords in AD Description Fields

OFFICE 365 SECURITY

- Conditional Access Policies
- Auditing Configuration
- Identity Security Score
- App Security Score
- Data Security Score

ACTIVE DIRECTORY

- Active Directory Certificate Templates
- Machine Account Quota
- LDAP Anonymous Access
- Domain Controller
- KRBTGT Password Age
- Discretionary Access Control Risks

COMMON CONTROLS

- Web Content Filtering
- Network Intrusion Detection
- Email Content Filtering
- Firewall Security Zones and Filtering
- Security Event and Alarm Monitoring
- Backups
- End User Awareness
- Mobile Device Mgmt.
- Internal MFA (Servers)

ACCOUNT SECURITY

- Least Privilege
- Group Policy Script ACLs
- Tiered access
- Dormant AD Accounts
- Network Share Privilege Review

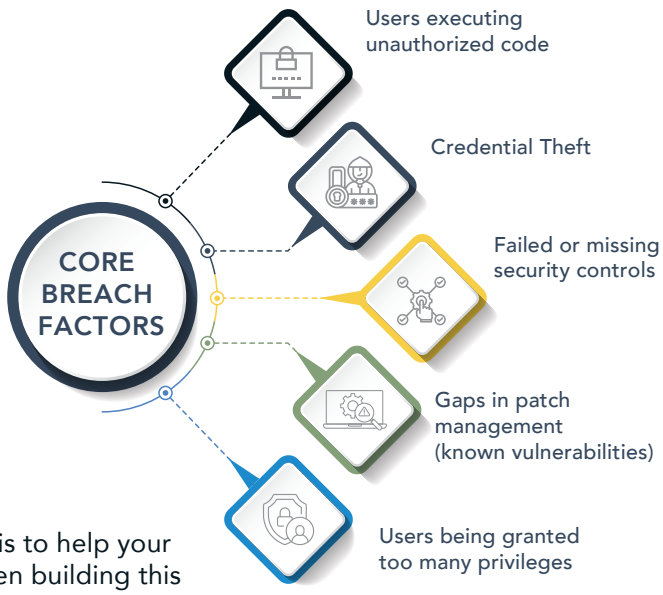
ENDPOINT SECURITY

- Malware Protection
- OS Hardening
- Endpoint Protections
- Vulnerability Analysis
- Unauthorized AI Agents

EXTERNAL SECURITY

- Vulnerability Analysis
- Attack Surface
- Authentication
- Reputation Analysis

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 is 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.

DEANDORTON

Cybersecurity Scorecard – Threat Alignment

How our seven assessed security domains map to every stage of a real-world ransomware attack–turning complex security data into a clear, measurable posture score.

7 SECURITY DOMAINS | **49+** CONTROLS ASSESSED | **12** KILL CHAIN PHASES

WHAT ATTACKERS DO	WHAT WE MEASURE	WHAT YOU GAIN
1 Get In Phishing emails, exposed RDP, unpatched services, & weak or stolen credentials give attackers their first foothold. *64% of SMB ransomware starts here*	**EXT External Security** Vulnerability scanning · Attack surface review · External MFA **CC Common Controls** Email filters & sandboxes · Web content filtering · End-user awareness **365 Office 365/Cloud** MFA Security · Conditional Access Policies · MSTeams Security	**CLOSES ENTRY POINTS** Patched perimeter, enforced MFA, filtered email & trained users eliminate the most common initial access vectors.
2 Run Malware & Stay Hidden Payloads execute via macros, PowerShell, or trusted system tools–then persist through scheduled tasks, registry changes & dormant accounts. *Avg. 258 days before detection*	**EP Endpoint Security** AV/EDR & tamper protection · OS hardening (MSCT) · Macro & script blocking · Patch management · Unauthorized AI agent detection **ACC Account Security** Dormant account review · Logon script security **CC Common Controls** Security event monitoring · App consent policy review	**STOPS EXECUTION & PERSISTENCE** EDR blocks malicious code. Macro controls prevent document-based delivery. Monitoring surfaces activity before a foothold is established.
3 Gain Admin Power & Steal Credentials Attackers exploit excessive privileges, misconfigured AD & weak passwords to escalate from a standard user to domain administrator. *One stolen credential can unlock the entire domain*	**ACC Account Security** Tiered admin access · Least privilege & local admin audit · Network share privilege review **PWD Password Security** Weak password audit · LAPS/local admin PW mgmt · GPP & exposed credential scan · Browser saved credential exposure **AD Active Directory** DACL Security · ADCS Security · LAN Manager authority level	**BLOCKS ESCALATION & CREDENTIAL THEFT** Tiered admin boundaries, LAPS & AD hardening remove the pathways from a single compromised account to full domain control.
4 Spread, Collect & Exfiltrate Attackers map the network, move laterally via RDP & SMB, harvest sensitive files, then beam data out through encrypted channels. *Data theft enables double-extortion demands*	**CC Common Controls** Network IDS/IPS · Firewall zones & egress rules · Security event monitoring · Internal MFA (servers/RDP) **AD Active Directory** LDAP anonymous access · DC hardening **365 Office 365/Cloud** Audit log retention · Data security score · Conditional access policies	**DETAINS & CONTAINS SPREAD** NIDS, firewall segmentation & MFA-protected servers slow lateral movement & flag anomalous transfers before significant damage occurs.
5 Deploy Ransomware Files are encrypted, backups targeted for destruction & ransom demands arrive–often with a timer & a threat to publish stolen data. *Median ransom: $170K–$200K (not counting downtime)*	**CC Common Controls** Backup security **EP Endpoint Security** EDR behavioral detection · Ransomware rollback capability **EXT External Security** Reputation & dark web monitoring	**ENABLES RECOVERY–WITHOUT PAYING** Immutable offline backups independent of AD ensure recovery even after full domain compromise–removing the attacker's leverage entirely.

DEANDORTON

Turn Complex Security Data into Actionable Insights

Simply measuring issues one by one isn't enough. What sets Dean Dorton's Cybersecurity Scorecard apart is its ability to correlate observed security gaps at the host level–giving organizations a clear picture of where the greatest risks truly lie and enabling rapid, targeted action.

Example:
An outdated antivirus definition alone may seem minor, but combine that with multiple critical vulnerabilities and a user with local admin rights, and you've got a high-risk asset that demands immediate attention.

Context Matters:
While individual assets may pose risks, your organization's layered defenses–such as email and web filtering–can significantly reduce overall exposure. Understanding this balance is key.

Why Dean Dorton is Different:
Our Cybersecurity Scorecard goes beyond surface-level checks. Using data collected from inside and outside your network during on-site assessments, we add critical context through interviews with system administrators to evaluate shared controls and layered defenses.

By combining account, endpoint, and external intelligence, we deliver a ***high-level view of your organization's risk posture against common threat actor tactics***–and show where your efforts will have the greatest impact.

This insight is essential for prioritizing actions, improving your security posture, and reducing risk efficiently.

Michael Gilliam
Cybersecurity Risk & Compliance Senior Manager
859.425.7794
mgilliam@deandorton.com