CYBERSECURITY ASSESSMENT SERVICES

How confident are you that your digital assets are adequately protected?

Dean Dorton's cybersecurity assessment services provide your organization with specific information about the state of your cybersecurity posture and validate that key controls are working as expected. We offer a variety of services to accommodate any of your requirements, network architecture, and business scenarios.

Our methodology follows project management best practices so at any point in time during the project you know its status, the next steps, and when you will receive your security assessment report.

OUR COMMITMENT TO YOU:

Deliver an easy-to-read cybersecurity assessment report with insightful and actionable information, all in a timely manner by the agreed upon deadline.

External Security Assessment

Internal Security Assessment

Adversarial Threat Simulation (Penetration Testing)

Application Security Assessment

Cloud Security Review

Mobile Devices Security Review

TECHNOLOGY CONSULTING
DEANDORTON
DEAN DORTON ALLEN FORD, PLLC
BUSINESS ADVISORS CPAs CONSULTANTS

Gui Cozzi • Cybersecurity Practice Lead
859.425.7649 • gcozzi@ddaftech.com
deandortoncyber.com

48%

Percentage of breaches that feature hacking.

2018 Data Breach Investigations Report (Verizon)

83%

Percentage of the Internet of Things (IoT) devices sampled that have critical vulnerabilities.

2018 Annual Cybersecurity Report (Cisco)

54%

Percentage of new mobile malware variants that increase in a year.

2018 Internet Security Threat Report (Symantec)

95%

Percentage of cloud security failures projected through 2022 to be the customer's fault.

Is the Cloud Secure? (Gartner)

CYBERSECURITY ASSESSMENT SERVICES

External Security Assessment

The External Security Assessment is performed from outside your organization's security perimeter, usually from the Internet. The assessment can also include optional Social Engineering Testing to see how likely users fall to phishing and other scamming techniques used to start cyberattacks which often result in data breaches.

Objectives:

- Identify all known systems and network vulnerabilities that could be exploited by an external hacker
- Meet security assessment requirements for regulated entities (this is now common practice across all industries)
- Recommend additional controls to improve your external cybersecurity posture

Internal Security Assessment

The Internal Security Assessment is conducted from your organization's internal network to identify vulnerabilities on internal systems. In addition to vulnerability identification, this assessment also encompasses deep-dive security reviews of specific areas to include security configuration management, hardening, and best practice reviews.

Objectives:

- Show the damage that a hacker who has gained access to the internal network can inflict
- Meet security assessment requirements for regulated entities (this is now common practice across all industries)
- Recommend additional controls to improve your internal cybersecurity posture

Adversarial Threat Simulation (Penetration Testing)

Adversarial Threat Simulation (also known as Penetration Testing or Red Teaming) mimics real-world cybersecurity attacks. This involves real attacks on real systems and data, leveraging tools and techniques used by hackers.

Objectives:

Dean Dorton will work closely with your organization to select a specific scenario that makes the most sense based on your specific risk. Examples include:

- Gain access to specific internal systems from the Internet without being authorized
- Obtain privileged access, such as Domain Admin
- Access sensitive information and demonstrate that data extraction is feasible
- Recommend additional controls to minimize the likelihood of a successful cyberattack

Web Application Security Assessment

The Web Application Security Assessment provides an in-depth examination of various types of applications. Our review is based on guidance provided by the Open Web Application Security Project (OWASP) and industry best practices. Optional assessment modules include the review of Mobile Applications.

Objectives:

- Determine if the application is leaking sensitive information
- Identify as many potential security issues that could be exploited to gain access to sensitive data or systems
- Assess whether the application is susceptible to Denial of Service attacks
- Support you in developing and maintaining secure applications
- Recommend controls to improve application security and resilience

Cloud Security Review

More organizations are moving some or all their IT infrastructure and critical data to the cloud. Each cloud solution requires that specific configuration settings be enabled in order to ensure that the data and systems are protected from unauthorized access.

Objectives:

- Review security configuration settings of cloud storage such as Microsoft Azure/O365, Amazon Web Services, or Google Cloud Storage
- Recommend configuration settings or additional controls to maintain the confidentiality of the data stored in cloud environments

Mobile Devices Security Review

Dean Dorton will leverage the Mobile Devices security recommendations from NIST SP-124 to review a sample of devices. We'll look for adherence to policy as well as risks associated with data communication and storage, user and device authentication, and applications.

Objectives:

- Review existing Mobile Devices policy to understand your organization's objectives
- Verify through testing that expected Mobile Devices controls are effective
- Recommend controls to minimize the risk of data loss or theft on Mobile Devices