

Securing information and eliminating vulnerabilities without hindering students desire to explore and learn

Security



At a Glance

The University of Dayton stands as a leader in higher education and one of the preeminent Catholic universities in the nation. It's the largest private university in Ohio.

Founded by the Society of Mary in 1850, the university focuses on educating the whole person through a community of challenge and support. A University of Dayton education is transformative. Students are prepared for both life and work, and learn skills in building community.

The University of Dayton has a deep commitment to academic excellence offering more than 70 high-quality programs at the undergraduate level in four accredited divisions and provides premiere graduate programs at both the master's and doctoral levels. UD offers a law degree, either traditional or accelerated.

Recognized as a top-tier university, the University of Dayton offers the resources of a large university and the personal attention of a small college.

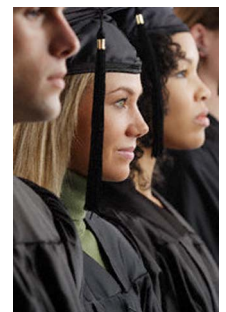
The Challenge

When the identities of eight students were inadvertently exposed on the Internet, the University of Dayton determined that it might have more areas that could be compromised within its network. Although certain of the security of its core systems, the University wanted to verify the security of all of its systems. Being an educational institution requires the University to operate with availability to many constituencies and that adds complexity and risk to their IT environment.

The Solution

A security assessment performed by Digital Controls, an objective third party, provided the University with an unbiased, comprehensive overview. Hacker methodologies were used to determine vulnerabilities. The risk associated with these vulnerabilities was assessed against best practices. Based upon the findings and conclusions, an Action Plan was created for the University - prioritized by greatest risk, rapid mitigation, costs, and capabilities. IT risk was constantly measured against what was reasonable. This provided the University with a secure but functional network.

Security is a process, not a product with a lifecycle - consisting of assessment consulting, implementation, and testing.



The Result

- *Restructured the network architecture to improve overall security – securing all systems on the network.*
- *All systems were reconfigured to eliminate the running of any unnecessary services*
- *Hired full-time Risk Management Officer to maintain strong security posture*

The University of Dayton has leveraged the Digital Controls assessment to bolster its IT security and will continue to verify its security level through constant diligence and periodic assessments.

Security Assessment Services

Scope

In today's business climate, your network infrastructure is one of the most crucial resources within your organization. It's imperative that it is consistently available and safe for your personnel to remain productive.

Network threats are prevalent with the barrage of daily hacking attacks - via spyware, malware, viruses, rogue points, weak passwords, denial of service, etc...

A third party security assessment allows you to feel confident that you've not overlooked a potential gap in your network infrastructure which can compromise your business - which severely hinders your being able to conduct

business or potentially leading to work stoppage.

A security assessment validates the systems that are externally accessible, determines the vulnerabilities posed by these systems, allows for further assessment of the risks vulnerabilities pose, and recommends how to best mitigate the vulnerabilities identified.

The primary purpose of a security assessment is to test current practices, verifying the security posture of your organization to ensure a best practices approach is in place.

How can you determine if your company has a secure best practices posture?

Here's how it works:

- Foot printing; gathering of external information to begin development of the plan of attack - includes identifying IP addresses, phone numbers, personal contact information, and other accessible information outside your network in the public domain
- Enumeration reconnaissance of system and network; performance of external network scans and ping sweeps to determine the types of systems, services running, and vulnerabilities that be exploited
- Exploitation; vulnerabilities attacked using hacker methodology tools and techniques seeking to determine vulnerabilities in your external systems allowing for penetration into internal systems and/or devices
- Executive briefing; presentation of detailed documentation of actions and findings
- Action plan; developed remediation recommendations prioritized and actionable to mitigate risk and secure your organization's systems