While mobile, cloud and virtualization has led to enhanced business productivity it has also led to new attack vectors that provide lucrative targets for malicious actors. With more devices and systems connecting to organizations’ networks the security conversation has changed dramatically. It’s no longer a question of if but when the network will be breached.

Traditional perimeter defenses can no longer be relied on as the sole means of protection. Organizations are implementing advanced security technologies for all aspects of the network including: the network edge, the data center, the enterprise LAN and externally connected computers.

Iron Bow Technologies works with organizations to implement these technologies to achieve resiliency. We design and implement security solutions that directly correlate to how users access and use data to provide protection against today’s advanced attacks.

**NETWORK VULNERABILITY ASSESSMENTS**

You don’t know your greatest weakness unless you are looking for it.

With all of the new security technologies being deployed across the network it is more important than ever to have a holistic look at the security of the network. Network vulnerability assessments are an important component of continuous monitoring to proactively determine vulnerability to attacks and provide verification of compliance with security best practices.

An Iron Bow Network Security Assessment provides a way to take control and proactively mitigate organizational risks before trusted assets and critical business continuity are compromised.

The assessment includes the following examination:

- **The State of the Network**: How easy is it to perform unauthorized activity in key segments of the network? Are there any serious or long-term vulnerabilities?
- **Current security capabilities**: How does your staff detect and respond to incidents? How do they determine if and where vulnerabilities exist? Are these methods or tools effective?
- **Policies and procedure effectiveness**: How are you currently evaluated on PCI, HIPPA, STIG, FISMA or other regulatory guidelines? Are your policies having the intended results? Are you able to maintain and enforce the regulatory guidelines?
- **Threats and impacts unique to your organization**: What are the potential threats to your assets? What is the probability of a breach? What assets are at risk? What is the cost of a compromise?
- **Balancing the risk**: What is the right balance between business needs and security risk for your organization?

The four phase approach allows us to answer all of these questions and more.

**Phase 1: Discovery**

- Project kick-off
- Review business goals and challenges
- Review of system and network operations
Phase 2: Data Collection
- Interview stakeholders
- Evaluate the state of the network
- Review baseline results from existing security controls and prior assessments
- Review security policies and procedures
- Perform a network vulnerability scan

Phase 3: Analysis
- Analysis of vulnerability scan data
- Analysis of existing network topology, controls and configurations
- Processing through best practices and compliances matrix

Phase 4: Presentation
- Executive presentation by Iron Bow cyber security consultants
- Assessment Report – actionable prioritized report of discovered vulnerabilities and gap analysis based on best practice and compliance standards with a timeline based recommended plan of action
- Assessment Results – raw data gathered during the assessment informs the assessment report and creates a snapshot that can be used as a baseline to track subsequent security posture improvement
- Executive Summary – customer presentation providing an overview of the assessment findings and a strategic roadmap enhancing security posture based on organizational risks

This proactive action reduces the possibility of successful attacks against important assets that could lead to loss of intellectual property, reputation and money.

IRON BOW IN ACTION

Most organizations have well-defined security practices that have been in place for years without a major incident. This does not mean that they are completely secure. Our vulnerability assessments take a deeper look at network traffic to discover anomalies that may not impact performance or security today, but pose a threat nonetheless. In one case, we discovered, through a combination of raw data and user interviews, a customer was open to malicious actors via several well-known and well-used workarounds. The weakness had not been targeted yet, but posed a huge risk. Iron Bow provided a detailed network vulnerability assessment and was able to lay out a prioritized plan for increasing the client’s security posture that dramatically shrunk the potential attack vectors, increased visibility and stayed within budget.

Iron Bow has the expertise and experience to understand organization use cases, recommend the best solution and ensure that the solution is successfully deployed in an operationally sustainable method.

**STRONG.** Data analytics and personnel interviews combine to provide full picture of how data and systems are accessed.

**FLEXIBLE.** Our assessment takes into account organizational policies and procedures to ensure that security remains an enabler.

**TARGETED.** Resiliency is the goal of all engagements. Our assessments show how best to mitigate risks across the network so that key assets and business continuity are never threatened.