Cooper Consulting

Cybersecurity

Assessment and Compliance

Whether you are concerned about your security architecture and controls or evaluating existing policies and procedures, Cooper Consulting and our partners can identify potential vulnerabilities in your current security program.

EVALUATIONS

We can evaluate the security of your system from multiple points of view to ensure that your security strategy is working properly. Evaluations can be performed from multiple locations within and outside your network. This allows us to thoroughly understand and explain the threats from each attack point to ensure the best return on investment for security and functionality.

OUR PROCESS

We start by conducting risk and vulnerability assessments to identify deficiencies:

Evaluate. We perform an in-depth review of your current incident response plan, including roles and responsibilities, internal and external response capabilities, and other security controls.

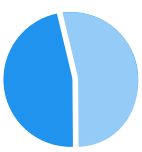
Analyze. We compare your existing plan against best practices and our first-hand experience to determine gaps, potential response issues, and recommendations for remediation.

NO SURPRISES!

CORRECT IMMEDIATE THREATS

Test. We conduct practical exercises to assess and validate your incident response team's readiness.

Report. At the end of the engagement we provide a comprehensive report that highlights key findings, identifies gaps in your incident response capabilities, and provides recommendations on how to correct or enhance your plan to strengthen your security posture.



52%

of State agency CIO's documented the effectiveness of their cybersecurity program with metrics and testing in 2015.

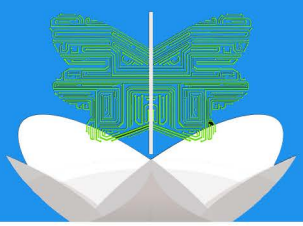
Source: October 2015 NASCIO The Value Equation Survey

OUR CLIENT SPECIFIC APPROACH

Cooper acts as outside counsel to ensure you have an objective view of your security posture and IT risk management strategy.

Our assessment includes:

- **Independent advice based on best practices.**
- **Delivering the capabilities you need for information security and assurance.**
- **Working with your team and your budget to develop, evaluate and implement a cyber security policy.**



Email: cooper@cooperconsulting.com
Phone: 512.527.1000
www.cooperconsulting.com

REPORT AND ESCALATION

At the conclusion of the assessment, we provide you with a final report that includes a detailed analysis of the findings, along with recommendations on how to strengthen your security posture.

ACTIONABLE RECOMMENDATIONS

All findings are rated based upon their risk, the probability of exploitation and the potential business impact. This allows our clients to focus their efforts on mitigating the risks that matter the most.

By combining known threats, architectural design, and the probability of occurrence with risk transference strategies, we're able to provide a clear representation of an organization's risk posture.

On average, it takes 229 days

THAT'S ALMOST 8 MONTHS!

before a company realizes it has been hacked. And 67% of the time, it can't even determine that itself; it has to call in an outside consulting firm.

Source: http://www.businessinsider.com/why-youre-more-likely-to-get-hacked-on-wednesday-2015-2

23%

of State agency CIO's stated lack of visibility and influence with the enterprise as a major barrier.

Source: October 2015 NASCIO The Value Equation Survey