



CYBER SECURITY CONSULTING SERVICES

We help companies understand and solve the challenges of cyber security so they can focus on more important things—growing their business!



**The Intellection
Group, Inc.**

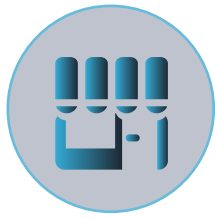
THE DATA SIMPLY CAN'T BE IGNORED!

When you combine the incidents involving malicious and inadvertent insiders, they dwarf any other computer security threat. According to a recent study, among 874 incidents, 65% were caused by employee or contractor negligence; 10% by outsiders using stolen credentials; and 22% by malicious employees and criminals.

Industries We Serve



HEALTHCARE



RETAIL



GOVERNMENT



EDUCATION



TELECOM



FINANCIAL

HOW WE WORK

- Extensive experience with Investor and M&A due diligence assessments of cyber risk
- Executive engagement and experience with Homeland Security infrastructure
- Immediate response time for critical projects
- Managed Services offerings to ensure on-going security upgrades and policy compliance



OUR CYBER SERVICES: 6 KEY PRACTICE AREAS

1.

IDENTITY & ACCESS MANAGEMENT

Ensuring that the right people have access to the right resources at the right times, and for the right reasons.

2.

VENDOR RISK & SECURITY MANAGEMENT

Many recent high-profile government and corporate security breaches have stemmed from this difficult to control vector.

3.

PENETRATION TESTING

A multi layer process of automated + manual scanning of networks, systems, apps, and access portals.

4.

INSIDER THREAT MANAGEMENT

Risks from malicious and inadvertent insiders dwarf any other computer security threat that your company faces.

5.

FACILITIES SECURITY

Physical access control of your offices and business systems from intrusion and intentional damage or theft.

6.

REPUTATION MANAGEMENT

Need help because you didn't have a Cyber Security plan in place, and ended up in a crisis? We can put a recovery plan in place.

IT CAN HAPPEN TO YOU

One of the biggest areas of risk around the value and stability of a business in today's corporate environments, however, is often overlooked—or simply just taken for granted: the high risk (and high probability) of incurring Data Breaches and Cyber Security Attacks. This is often an oversight in proper executive leadership, aggravated by short-term priority setting, and lack of proactive participation in cyber risk management. Regardless of the root cause - no organization should consider themselves safe.

TAKE THE FIRST STEPS TO PROTECT YOUR ASSETS

So what can you do to educate yourself and take proactive steps to ensure these concerns are addressed? The Intellection Group offers select executive teams concerned about these topics a C-suite briefing on the current status of cybersecurity. The high level briefing is an excellent way to increase awareness of cybersecurity issues and bring corporate executives to a common understanding of cyber threats and mitigation management approaches.

THE EXECUTIVE BRIEFING FOCUSES ON 7 MAIN TOPICS

 2018 CyberSecurity Trends	 Incident Reviews of Recent Cyberattacks in the Financial Services Industries	 Primary Threats to Financial Services Industries	 Why Financial Services is a Specific Target of State Actors and Cyber Criminals
---	--	---	---

 Current Financial Services Industry Initiatives in CyberSecurity	 Best CyberSecurity Practices for the C-suite	 Methodologies for Developing & Implementing C-level Policies and Strategies
--	--	---

If you'd like to learn more, please [contact us](#) for a confidential discussion and more information on the Executive Briefing opportunity.

CONTACT US



Telephone
678-283-4283



E-mail:
dbernard@intellectiongroup.com