A Comprehensive Guide to

Security Advisory Services

FROM THE MANAGED SERVICES EXPERTS AT TPx

Executive Summary

The volume of businesses' digital assets is growing with increasing velocity, as are cyberattacks. At the same time, the number of cybersecurity specialists is shrinking at an alarming rate.

To fill this widening gap, businesses of all sizes and types are partnering with security experts. Security Advisory Services provide companies with the cybersecurity assessments and solutions they need.

This guide introduces Security Advisory Services and how they can help businesses navigate an ever-changing threatscape.

Key Takeaways

- Security Advisory Services can help businesses uncover network vulnerabilities and cybersecurity gaps.
- Security Advisory Services can bolster incident response capability and minimize the impact of a possible attack.
- A key byproduct of Security Advisory Services is an increase in customer trust.
- With Security Advisory Services, even small companies can ensure regulatory compliance and client privacy, allowing them to compete for larger customers.
- Working with a trusted Security Advisory Services provider can give businesses instant access to expertise and quicker time to value without adding overhead.

Table of Contents

PART 1:

What Are Security Advisory Services?

Cyberthreats are growing in number and sophistication every day. When your business is ready to increase the protection of networks, endpoints, employees and data from impending cyberattacks, it's sometimes difficult to decide where to start.

Security Advisory Services from third-party security specialists can help uncover your business's vulnerabilities and recommend optimal security. Working with a trusted Security Advisory Services provider not only enables your company to access the most current and specialized cybersecurity knowledge, but it also expands your existing IT team with tech talent that is hard to source.

Security Advisory Services provide enterprises and SMBs with a cost-effective way to:

- Access cybersecurity expertise that's expensive and challenging to recruit and retain
- Understand your company's vulnerabilities and identify gaps in your cybersecurity
- Define a cybersecurity strategy
- Bolster incident response capabilities and mitigate risk
- Minimize the impact of and facilitate recovery from attacks
- Sustain long-term security policies

Security Advisory Services also come to the rescue when it comes to compliance. Security Advisory Services providers are well-versed in regulations issued by organizations, such as the:

- Federal Trade Commission (FTC)
- Federal Communications Commission (FCC)
- Cybersecurity & Infrastructure Security Agency (CISA)
- National Institute of Standards & Technology (NIST)

Security Advisory Services can help enterprises:

- Prepare for audits
- Comply with security regulations
- Free up overburdened IT security teams

How Do Security Advisory Services Work?

Security Advisory Services are tailored to meet the unique needs of each organization, helping them to strengthen their defenses against cyber threats and mitigate risks. The beauty of working with a Security Advisory Services partner is having almost immediate access to exceedingly thorough, timely and actionable cybersecurity advice. Nearly all Security Advisory Services engagements involve some type of assessment to zero in on the customer's needs.

What Elements Are Included in Security Advisory Services?

Security Advisory Services can vary from one consultant or provider to another. However, some common offers include the following:

- Cybersecurity Gap Assessment
- Network Vulnerability & Penetration Scanning
- Network & Wireless Security Assessments
- Policy Definition & Creation
- Ransomware Readiness Assessment
- Virtual Chief Information Security Officer (CISO)
- Audit Preparation
- Incident Response Planning
- Security Awareness Training
- Compliance Management

PART 2:

Why Should Businesses Invest in Security Advisory Services?

Fortinet's 2022 Cybersecurity Skills Gap Report states that 80 percent of organizations experienced one or more cybersecurity breaches during the last 12 months. Attackers are getting smarter, and attacks are becoming more frequent. It's no surprise that increasing numbers of businesses are turning to security advisors for help.

The global Security Advisory Services Market was valued at $11.1 billion in 2021 and is expected to grow nearly four-fold, reaching $41.4 billion by 2032, reveals **Future Market Insights** (FMI). Businesses realize that incurring and recovering from a cyberattack can be extremely costly and possibly damage their companies – or their reputations – beyond repair.

Here are some reasons your business should consider engaging Security Advisory Services:

Reduce Risk of Cyberattacks

According to **CNBC's Momentive Q3 2021 Small Business Survey**, 42 percent of small business owners have no cyberattack response plan. Employing the help of a Security Advisory Services partner will help expose vulnerabilities in your network – no matter the size or type of your business – and enable you to mitigate cybersecurity risks.

Protect Sensitive Data & Mitigate Risk

If your business has employees, it has sensitive data. Add to that customer, client or patient data and the sensitive data grows exponentially. Security Advisory Services can protect your data — whether it's HR files or intellectual property — from unauthorized access, breach or theft.

Meet Regulatory Requirements

If your business is in a regulated industry, it's subject to specific data security requirements that, if not met, can result in steep fines and reputational damage. Security advisors can help protect your business from inadvertent – and potentially costly – violations.

Improve Customer Trust

A demonstrated commitment to data security assures customers that your business has their best interests at heart. As cyberattacks increase, customers are more aware of and interested in how proactive your company is in protecting their data.

Enhance Business Continuity

Planning for an attack is smart business, and Security Advisory Services experts can help you do that. Being prepared is the best defense and guarantees that you will minimize disruption and damage to your business in the event of a breach.

Minimize Impacts of an Attack

Security Advisory Services can prepare you to respond proactively and effectively in the event of a cyberattack. Experts can customize a plan to minimize downtime, business loss, cost and reputation damage.

Get Cyber Insurance Coverage

As attacks have become more commonplace, cyber insurance coverage will only be eligible to companies who follow cyber defense procedures and polices, which a Security Advisory Services provider can help your company implement.

Risk Identification & Prioritization

Security Advisory Services enable you to mitigate risk to your organization by conducting a Cybersecurity Gap Assessment. This assessment uncovers where you're most vulnerable and how to prioritize the implementation of security solutions.

80 percent of organizations experienced one or more cybersecurity breaches during the last 12 months.

PART 3:

What Should Businesses Look for in Security Advisory Services?

Not every Security Advisory Services provider or cybersecurity consultant is equal. If your company is looking to augment its security policies, procedures, plans and protections, you may seek advisors that seem to offer the most services. However, digging deeper into a Security Advisory Services provider's solutions and expertise will help ensure you're working with the right provider.

What Are Key Considerations in Selecting Security Advisory Services?

Your business should look for the following components in a Security Advisory Services partner:

Knowledge + Hands-On Experience
Does the provider have real-world experience managing security solutions and up-to-date knowledge on how to advise during a breach? Choose a provider that's staying in the loop on current trends and is immersed in the industry.

Information Security Standards Adherence

Does the advisor follow established standards provided by:

- National Institute of Standards & Technology (NIST)
- Certified Information Systems Security Professional (CISSP) Domains
- ISO 27000 Series
- Vertical-specific compliance (HIPAA, CISA, PCI-DSS, etc.)
- FTC Safeguards Rule

Solution Prioritization

No organization can roll out every cybersecurity solution all at once. Will the advisor use assessments to identify the most vulnerable parts of your network and prioritize solution deployment? Or will you be pressured to deploy solution after solution without regard to your budget, organization size and specific needs?

Ongoing Accountability

Is the solution provider going to be around in the event of a breach on your organization in the future? Or will they come in, recommend technology and then disappear, leaving you to handle day-to-day defense of your company?

Team Expertise

Does the provider have the proper credentials and experience to advise your business? Can they share success stories or case studies with other clients?

Monitoring + Governing

Work with a provider that recognizes the importance of ongoing monitoring and governance to protect from future cyberattacks.

Field Testing

Security Advisory Services should involve several tests of your network's vulnerabilities. Will the provider test the entry points of your network? Will they test your employees' responses to simulated attacks? Will they use social engineering tactics – like people posing as techs to get onto the premises – to test your defenses?

Flexibility

Will your Security Advisory Services provider be attentive to changing requirements – new devices, applications, services or threats? And will they be proactive in integrating new technology or solutions to consistently enforce your defense?

Training

What types of training are provided? Does the advisor offer videos, webinars or other learning management system (LMS) items to make security training accessible and engaging for your employees?

Pricing

Can the provider offer flexible pricing models that work for your business? Is the pricing monthly, annual or project-based? Are assessments and solutions priced per user or device?

Certifications & Compliance

Does the provider have the certifications or compliance needed to excel in your industry?

- Payment Card Industry Data Security Standard (PCI DSS) for payment cards
- Health Insurance Portability and Accountability Act (HIPAA) for healthcare data
- Federal Information Security Modernization Act (FISMA) for federal contractors
- **National Institute of Standards and Technology** (NIST) for general network security
- Service Organization Control (SOC) for cybersecurity risk management

What Are Common Mistakes Made in Selecting Security Advisory Services?

When selecting Security Advisory Services, businesses tend to make these mistakes:

Mistake 1
Going with a “cheaper” option that isn’t suitably qualified.

Mistake 2
Assuming your advisor is automatically going to help you with all technologies.

Mistake 3
Picking a provider that’s not versed in your business size, industry or regulations.

Mistake 4
Overlooking the level of service, including support and responsiveness.

PART 4:

Why Should Businesses Work with a Security Advisory Services Provider?

In the digital age, all businesses inevitably have vulnerability and/or compliance gaps in their network security environment. Your company has two options for addressing those gaps – take it on or work with a trusted partner, such as a qualified managed services provider (MSP).

Reasons to Work with a Provider

Lack of Expertise

The depth and breadth of knowledge demanded of IT teams today spans not only cybersecurity but data storage, data integrity, software development, information technology infrastructure library (ITIL), database design and management, network services, cloud computing, data analysis, troubleshooting and more. Security is a complex discipline and often requires specialized training and certifications.

Lack of Time

Due to the interconnected nature of integrated applications, devices and other technologies, IT departments are stretched thin putting out fires. One problem often leads to another, and the IT teams' work is never done. Many teams don't have time to handle thorough assessments, much less digest results and make strategic plans to address vulnerabilities.

Lack of Talent

The IT skills gap is a well-known challenge for businesses, especially SMBs, that cannot pay for hard-to-source cybersecurity expertise. Plus, there's still a global shortage of 3.4 million workers in this field, according to the **2022 (ISC)2 Cybersecurity Workforce Study**.

Despite adding more than 464,000 cybersecurity workers in the past 12 months, the workforce gap has grown more than twice as much as the workforce.

Working with an expert provider provides your company with:

Instant Access to Expertise
Working with an MSP delivers instant access to teams of trained personnel who are experts in protecting your business from cybercrime.

Reduced Overhead
You won't need to hire, retain or train cybersecurity specialists in-house since the MSP takes care of that process and expense.

The Ability to Focus on Your Business
Cybersecurity is a complicated undertaking and an entire business unto itself. A trusted partner allows you to focus on managing and growing your core business.

Competitive Advantage
With Security Advisory Services, even small companies can ensure regulatory compliance and client privacy, enabling them to compete for larger customers.

PART 5:

What Are TPx Security Advisory Services?

Need to amp up your online security but don't know where to start? The cybersecurity experts at TPx can help. We offer comprehensive security consulting services that can help improve your security posture and protect your business.

What are the Key Offerings of TPx Security Advisory Services?

Here are just a few offerings provided by the Security Advisory Services experts at TPx:

Virtual Compliance Officer (VCO), featuring a Gap Assessment

Imagine having a dedicated expert to navigate the complex world of compliance for your organization, without the need for a full-time, in-house officer. That's where our Virtual Compliance Officer (VCO) service steps in, offering you the perfect blend of expertise, flexibility and cost-effectiveness. With a gap assessment, continuous monitoring, and quarterly review, we help you identify, assess and mitigate compliance risks before they become issues.

Network Vulnerability & Penetration Scanning

Regular Vulnerability and Penetration Scanning are two of the best tools to understand where your weaknesses are and how likely a hacker will be able to exploit them. The Vulnerability Scan evaluates devices that are connected to the network for the purpose of identifying vulnerabilities that may be present on those devices due to open ports, exposed services, lack of current patches, etc. The Penetration Scan shows how exploiting a vulnerability could result in a significant impact.

Dark Web Monitoring

TPx's Dark Web Monitoring service operates around the clock, scanning thousands of websites from the digital underworld for indications of your data being compromised. Receive alerts when your data appears on the Dark Web.

Wireless Site Survey

The TPx Wireless Site Surveys service offers a comprehensive approach to optimizing wireless LAN deployments for businesses. It combines predictive modeling with on-site validation to ensure seamless wireless connectivity and performance. The service includes accurate coverage planning, interference analysis, and capacity planning, ensuring a robust network design that meets specific deployment requirements.

Network Security Assessment

Network security shouldn't be an afterthought or an "add on" to your existing network design. Without a fully integrated approach to network security, your business could be left at risk of cyberthreats and attacks. At TPx, we incorporate security considerations throughout the architecture assessment, yielding an extensive Network Security Assessment that results in actionable recommendations for a robust, high-performing and secure networking environment.

Wireless Security Assessment

Wireless networking enables work-from-anywhere flexibility and improves organizational productivity, but it also increases security risk and widens your attack surface. Our Wireless Security Assessment will examine your strategic and tactical wireless network configuration, focusing on areas that pose the highest risk of incidents and breaches to your business.

Ransomware Readiness Assessment

TPx's Ransomware Readiness Assessment (RRA) is founded on industry standards developed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). This assessment focuses on the aspects of cybersecurity that have the highest value in defending your organization against ransomware attacks. As a subset of TPx's full-blown Security Program Gap Assessment, the RRA provides a cost-effective way for small and medium businesses to understand the risk of ransomware to their organization.

Customized Security Advisory Services

The cybersecurity talent shortage is at an all-time high. Finding security experts is time-consuming, expensive, and in some cases, next to impossible. TPx can help bridge that gap with our team of security experts. We have broad experience in security and risk assessments, operations, architectures, policy compliance, privacy and many other security domains. We'll define and execute a tailored engagement and approach that meets your unique security requirements.

FTC Safeguards Advisory Services

The Federal Trade Commission's Safeguard Rules require financial companies to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The FTC Safeguards Rule identifies nine elements the program must include: Designate a qualified program owner, conduct a written assessment, design and implement safeguards, monitor and test program effectiveness, provide security awareness training, monitor service providers, keep the program current, document an incident response plan and report to your board of directors.

What are the Key Benefits of TPx Security Advisory Services?

- **Bridge the IT Skills Gap**
- **Effectively Manage Risk**
- **Focus on Your Business**
- **Adhere to Compliance & Regulatory Requirements**

PART 6:

Why Choose TPx?

You have enough business challenges. Partnering with TPx allows your IT staff to focus on your core business goals. At TPx, we have the products, services, experience and certifications to keep your network and applications running smoothly and safely.

Our mission is being the easiest MSP to do business with	We solve the biggest IT issues – cybersecurity, connectivity, and collaboration – under one umbrella	We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, Microsoft, SMC and more
We offer HIPAA, PCI-DSS, and SOC 2 Compliant solutions	We provide enterprise-class, 24/7 support	We offer different service levels and highly-customizble solutions
We have a national footprint, with multi-site, multi-carrier, partner coverage	With thousands of customers nationwide, we're big enough to get the job done and small enough to be agile	We have various dedicated teams to ensure service excellence
We continuously invest in automation, self-service innovation, and back-office transformation	We are committed to providing the most densely monitored service delivery platform in the industry	We understand and embrace the criticality of our customers' performance analytics

TPx is Your One-Stop Shop for Managed Security Services

Security Advisory Services

TPx Security Advisory Services provide comprehensive security consulting that can help improve your security posture and protect your business. Our services comprise a cybersecurity gap assessment, network vulnerability and penetration scanning, network security assessment, wireless security assessment and ransomware readiness assessment.

Security Awareness Training

Users are critical to keeping your organization secure. The more they know, the less prone they are to becoming victims of phishing scams or other security incidents. Our service includes monthly phishing simulations and Security Awareness Training courses with automated reporting to track your results.

Next-Generation Firewall (NGFW)

The firewall is the first line of defense in protecting your business from internet-based threats. Next-generation firewalls block today's advanced threats while providing secure access, visibility and control to help your business be more productive.

Endpoint Management and Security

TPx helps keep your servers and workstations healthy, secure and performing optimally. Our endpoint security service leverages remote monitoring and management (RMM), patch management and security. Together with expert support personnel and security analysts, we provide an "always-on," best-in-class, 24/7/365 service.

Managed Detection and Response (MDR)

Discover, prevent and recover from cyber threats faster. TPx's MDR helps you identify more threats, reduce attack dwell time, and proactively mitigate attacks. We offer managed detection and response for both firewalls and endpoints.

Unified Threat Management (UTM)

TPx ensures UTM features such as web filtering, antivirus, application control, intrusion prevention and VPNs are properly configured, monitored and maintained.

Managed Inbox Detection and Response (IDR)

Help users make better email security decisions with Managed IDR. This powerful user security solution provides professional evaluation and handling of suspicious emails reported by users — right from the inbox. Put your employees in the driver's seat and make them be part of your business security.

DNS Protection

We protect systems and users from malicious websites using leading DNS protection software. Windows devices are protected both on the corporate network and while traveling. Network-based DNS protection covers BYOD, guest wireless, and non-Windows devices to deliver comprehensive DNS security and reduce your risk of attack.

Backup and Disaster Recovery (BDR)

We help organizations quickly recover from system downtime and data loss caused by cyberattacks, human error, system failures and natural disasters. Using advanced hybrid local/cloud technology and skills management resources, TPx delivers a turnkey BDR solution that will meet your recovery objectives. All backups are scanned for ransomware and when a ransomware footprint is detected, you can roll back your systems as if it never happened.

Need Help with Cybersecurity or Compliance?

CONTACT US TODAY