



Quest Technology Sales Bootcamp Series

Understanding the Cybersecurity Landscape: Let's Get Real or Let's Not Play

Empowering Technology Advisors to Sell Cybersecurity with
Confidence

Your Host: Adam Burke

Vice President of Channel Partners and Sales



Quest. All Rights Reserved © 2024

October 9, 2024

Understanding the Cybersecurity Landscape: Let's Get Real or Let's Not Play

This series is designed to help you, as trusted advisors, confidently sell cybersecurity services—even if you're not a cybersecurity expert. As cyber threats evolve, businesses increasingly rely on their technology partners to guide them through the complex cybersecurity landscape.



We'll be covering:

- The current cybersecurity landscape and its significance in the IT ecosystem.
- Key strategies to qualify and identify client cybersecurity needs.
- An overview of Quest's CyberDefense Suite and how it integrates into broader IT strategies.



Knowledge You'll Gain:

- The importance of cybersecurity in today's market and its impact on business performance.
- How to confidently discuss cybersecurity services with clients, even if you're not an expert.
- Understanding how cybersecurity fits into and enhances broader IT solutions.



Skills You'll Gain:

- Techniques for qualifying client needs and determining the best cybersecurity solutions.
- The ability to position and sell cybersecurity services as part of a comprehensive IT strategy.
- Confidence in guiding clients toward the right cybersecurity solutions with Quest's support.



— Understanding the “Why” will propel your success!



Protecting Sensitive Data:

Businesses must secure personal, financial, and intellectual property data to prevent breaches that could lead to severe legal and financial consequences.



Compliance with Regulations:

Many industries are subject to strict regulatory requirements for data protection. Robust cybersecurity measures ensure compliance and avoid costly penalties.



Safeguarding Business Operations:

Cyber attacks can disrupt operations, leading to downtime and lost revenue. Effective cybersecurity ensures business continuity and minimizes the risk of operational disruptions.

Understanding the Cybersecurity Ecosystem and Services You Can Offer

Core Components:

Threat Prevention: Protecting against potential threats before they can cause harm.

Detection & Response: Identifying and responding to threats in real-time to minimize impact.

Compliance & Risk Management: Ensuring adherence to industry regulations and managing security risks effectively.

Service Categories:

Managed Security Services: Ongoing monitoring and management of security systems.

Consulting & Assessments: Expert guidance on improving security posture.

Integration & Implementation: Incorporating cybersecurity measures into existing IT infrastructure.

Tailored Solutions

Client-Specific Needs: Offer customized services that align with each client's unique challenges and objectives.

**Ransomware
motivated over 72% of
cybersecurity attacks
in 2023.**

Let's get real or let's not play

No Guessing | Quest's Opportunity Vetting Process

Key Points: Opportunity | Resources | Decisions

Next Steps:

How does the client decide to move forward?

- RFP
- Proposal
- Cheapest offering
- "Best Value"

Decision Makers

- Who is engaged in the decision?

Decision Process

- What is the process?
- How is this going to happen?
- By whom?

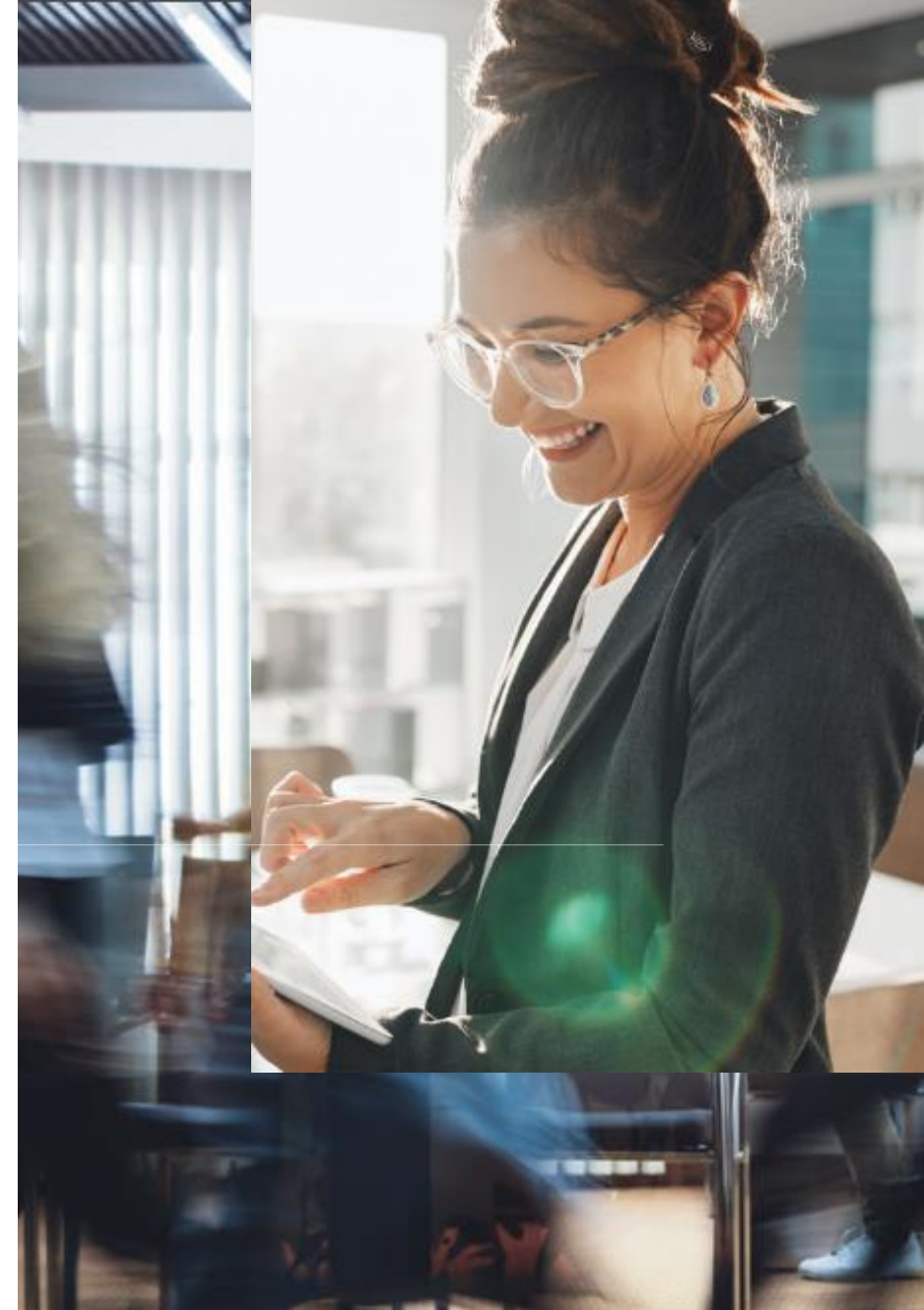
Execution

- What are the steps to the pain/problem being solved?

Discussing Cybersecurity with Your Clients Confidently

Key questions for the initial conversation

- **Pain:** What pain/problems are they trying to solve?
- **Urgency:** Is the pain/problem real?
- **Results:** What results does your client want?
- **Cost:** What is the cost of the pain/problem?
- **Solution:** Does your client have something they are already thinking about?



The Importance of Cybersecurity in Today's Market

Rising Threats: Cyber attacks are more frequent, sophisticated, and targeted than ever before. No organization, regardless of size or industry, is immune.

Preparedness and Response

- **83% of ransomware victims** paid the ransom in the wake of an attack.
- According to IBM, it takes an average of **49 days to identify a ransomware attack**.
- **35% of Chief Information Security Officers (CISOs)** are already using AI for security applications, **with 61% likely to use AI in the next 12 months**

Business Impact:

A breach can have devastating consequences, ranging from financial losses and significant reputation damage to regulatory fines and legal ramifications. The cost of inaction is far greater than the investment in robust cybersecurity.

Client Awareness:

Your clients are increasingly aware of these risks and seek trusted advisors to help them navigate this complex landscape. This is where you come in, equipped with the right solutions to meet their unique needs and protect their most valuable assets.



Quest's CyberDefense Suite

- **Comprehensive Protection**
Managed Security Services, Threat Detection & Response, Compliance & Risk Management
- **Tailored Solutions**
Flexible to fit client needs and existing infrastructure
- **Why Quest?**
Proven expertise and robust support to back your sales efforts

**Cloud environment intrusions
increased by 75% over the past year.**



Build Your Own Bundle:



Device Monitoring



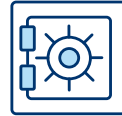
Endpoint Device Security EDR



ZTNA: Zero Trust
Network Access



DNS
Security



Password Protection



SIEM: Security Information &
Event Management



Email Security
Protection



Patch Management



Vulnerability
Scan/Attack Surface
Management



Immutable Storage



MFA: Multi-Factor
Authentication



Incident Response Services

Feature	IR T&M	IR Retainer	Readiness and Retainer	TOC
Service Level Agreements	Best Effort	1 hour by phone; 24 hrs onsite	1 hour by phone; 24 hrs onsite	4 hrs by phone; 48 hrs onsite
Service Model	T&M	12-mo Retainer	12-mo Retainer	12-mo Contract
Included IR Hours	Adhoc per Rate Sheet	160 hours annual	160 hours annual	T&M
24/7/365 Access to Incident Responders	✓	✓	✓	✓
Needed Response Tools (Quest EPS, SIEM, DNS Security)	✓*	✓	✓	✓*
Incident Coordination, Containment, and Investigation	Per Incident (T&M)	✓	✓	Per Incident (T&M)
Log, Host, and Network based Forensics as needed	Per Incident (T&M)	✓	✓	Per Incident (T&M)
Network Edge Vulnerability Scan	Per Incident (T&M)	Per Incident (T&M)	✓	Per Incident (T&M)
Annual 4-point Incident Response Readiness Assessment			✓	
I. Readiness Assessment			✓	
II. Environment Prep			✓	
III. Table Top Exercise			✓	
IV. Final Report			✓	
Proactive Threat Hunting / Compromise Assessment	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)
Internal IR, SOC, and Forensic Team Builds / Stand-up	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)
System Backup and Recovery	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)	Per Incident (T&M)

*SLA per Incident



Device Monitoring:

Quest keeps your firewall, IDS, and IPS devices updated and appropriately monitored 24/7, providing you with alerts and knowledge to handle any threat.



DNS as a Service (DNSaaS):

Quest provides a first line of defense against threats on and off the corporate network. We rapidly deploy our DNS enterprise-wide whenever you need it, blocking threats before they become attacks.



Email Security Suite:

Powered by Proofpoint, Quest helps you protect your people, data, and brand, no matter how complex your deployment is.



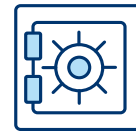
Immutable storage:

Quest stops bad actors from rewriting or deleting your backup data. Quest offers multiple service delivery centers to store immutable data.



Endpoint Detection and Response:

EDR services powered by AI. Our Endpoint Protection as a Service (EPaaS) provides reliable monitoring and alerts so you can handle suspicious events immediately.



Password Protection:

Our specialized security framework provides strong, easily-managed protection for all your data and systems. Quest's transparent guidance and compliance ensures your organization is safe and secure.



Patch Management:

Agent provides patching and remote access to help reduce support time and limit vulnerabilities related to patching.



Multi-factor Authentication:

MFA services provide endpoint protection and monitoring for advanced threats on all endpoints. Leverage our Incident Response team's extensive skills and capabilities and gain valuable insights.



Zero Trust Network Access

ZTNA services are a smart and easy way to grant access to your users while protecting your network and apps.



Security Information & Event Management:

SIEM software aggregates and analyzes log data generated throughout your infrastructure. You'll receive comprehensive reports on security-related incidents and events.



Vulnerability Scan/Attack Surface Management:

Quest provides external vulnerability assessments, enforcement of security policies, documentation of regulatory and policy compliance, and continuous monitoring for complete attack surface

How Cybersecurity Services Fit into a Broader IT Strategy

Cybersecurity: A Cornerstone of IT Strategy

Integral to IT: Cybersecurity is essential for maintaining a secure and resilient IT environment.

Foundation for Success: Enhancing Business Performance

Proactive Protection: Safeguarding IT systems supports business continuity and strengthens client trust.

Seamless Integration and Growth Opportunities

Holistic Approach: Cybersecurity naturally fits into broader IT strategies, complementing other tech initiatives.

Land and Expand

Introducing cybersecurity services opens doors for additional IT solutions, creating opportunities to expand your client relationship over time.

The average ransomware payout increased dramatically from \$812,380 in 2022 to \$1,542,333 in 2023.



Key Takeaways



Cybersecurity is Essential:

It's a critical component of modern IT strategies, and clients who need to protect their businesses are demanding it more and more.



You Don't Have to be an Expert to Sell Cybersecurity:

You can confidently sell cybersecurity services by understanding the basics and leveraging Quest's comprehensive solutions.



Quest is Your Partner:

Offering cybersecurity services meets an urgent client need and opens doors for expanding your service offerings and increasing revenue.

Top Ten Reasons Why You Should Be Selling Cybersecurity Services

Top 10 Reasons:

1. High Demand

Network and application security Total Addressable Market are both growing from 30+ Billion in 2023 to over 52 billion in 2025. Businesses are actively seeking cybersecurity solutions to protect their assets.

2. Critical Business Need

Cybersecurity is no longer optional; it's a fundamental component of any organization's IT strategy.

3. Revenue Growth

Offering cybersecurity services opens up significant revenue opportunities, including ongoing managed services and project-based work.

4. Client Trust

Helping clients secure their data builds stronger, long-term relationships based on trust and reliability.

5. Market Differentiation

Selling cybersecurity sets you apart from competitors who may not offer these essential services.

6. Comprehensive Solutions

Cybersecurity services complement other IT offerings, enabling you to provide a full spectrum of solutions.

7. Regulatory Compliance

Many industries are subject to strict regulations requiring robust cybersecurity measures—position yourself as the go-to advisor.

8. Client Retention

Providing essential cybersecurity services increases client retention by making you an indispensable partner.

9. Cross-Sell Opportunities

Cybersecurity opens the door to selling additional IT services and solutions, increasing your overall sales potential.

10. Protect Your Clients

Ultimately, you're helping to protect your clients from potentially devastating cyber attacks, securing their future and yours.



—
**Thank you for
joining us today!**

Would you like to learn more about Quest's capabilities?



Phone

+1800 – 326 – 4220



E-mail

Brittany_Owens@questsys.com



Quest

<https://questsys.com/>



Quest Partner Page

<https://questsys.com/Partners/>



Quest Partner Portal

<https://partnerportal.questsys.com/>



We hope you enjoyed today's webinar!

Check out our schedule below to register for our next one:



<https://lp.questsys.com/quest-partner-cybersecurity-bootcamp-series-overview>

