

IntegraONE

2024 OneCon

Managed Services

Streamline IT:

**We Manage Security, You
Lead Innovation!**

INTRODUCTION

In today's fast-paced digital landscape, maintaining security is essential – but it shouldn't be a burden that slows down your business. Our managed security solutions allow your team to focus on driving growth and innovation, while we handle the heavy lifting of keeping your environment secure and compliant.

We're here to **complement your existing IT team, not replace it.** By adding specialized resources and expertise, we help you achieve your goals faster more efficiently.

Dorie Juhasz

Service Operations Manager

BACKGROUND

10+ years working in Managed Service Industry

10+ years working in Manufacturing Industries

8+ years working in HealthCare Industry

Leadership in process optimization (ITIL)

Experience in ITIL, COBOT and NIST Frameworks

FUN FACT

Back in the early 90's, I worked for Pat Croce, when he sold his In-speech business to NovaCare (this was before he became the President of the National Basketball Association (NBA) Philadelphia 76ers)



WHY SECURITY MANAGEMENT IS CRITICAL

CyberSecurity Threats are Growing

Every business, large or small, is a target for cyber-attacks. Threats like ransomware, phishing, and data breaches can cripple your operations.

Compliance & Regulations

Whether it's GDPR, HIPPA, or any other regulatory framework, the stakes are high, and non-compliance can lead to severe penalties.

Airport Analogy



Checkpoints:

Just as TSA agents check passengers at every point, certified security experts ensure that vulnerabilities are addressed.

Advanced Detection:

Like scanners detecting hidden threats, our tools identify risks before they turn into full-blown crises.

Dedicated Experts:

TSA agents are specialized for their role. Similarly, our team brings deep expertise in cybersecurity, working around-the clock to keep your business safe.

HOW THE BAD GUYS GET IN



Phishing, web & ransomware



Compromised credentials



Weak passwords



Trust relationships & propagation



Poor encryption



Unpatched vulnerabilities



Misconfigurations



Malicious insiders



Zero day & unknown methods

BUSINESS CHALLENGES

- Shortage of Skills CyberSecurity Professionals
 - Overburdened IT Teams
 - Increased Complexity in IT Environments
 - Increased Attack Surface (BYOD & IoT)
 - Compliance & Regulatory Challenges
 - Data Privacy Concerns
 - High Cost of Security Tools
 - Balancing Budget with Security
 - Siloed Systems and Data
-

Managed Security Monitoring & Incident Response

01

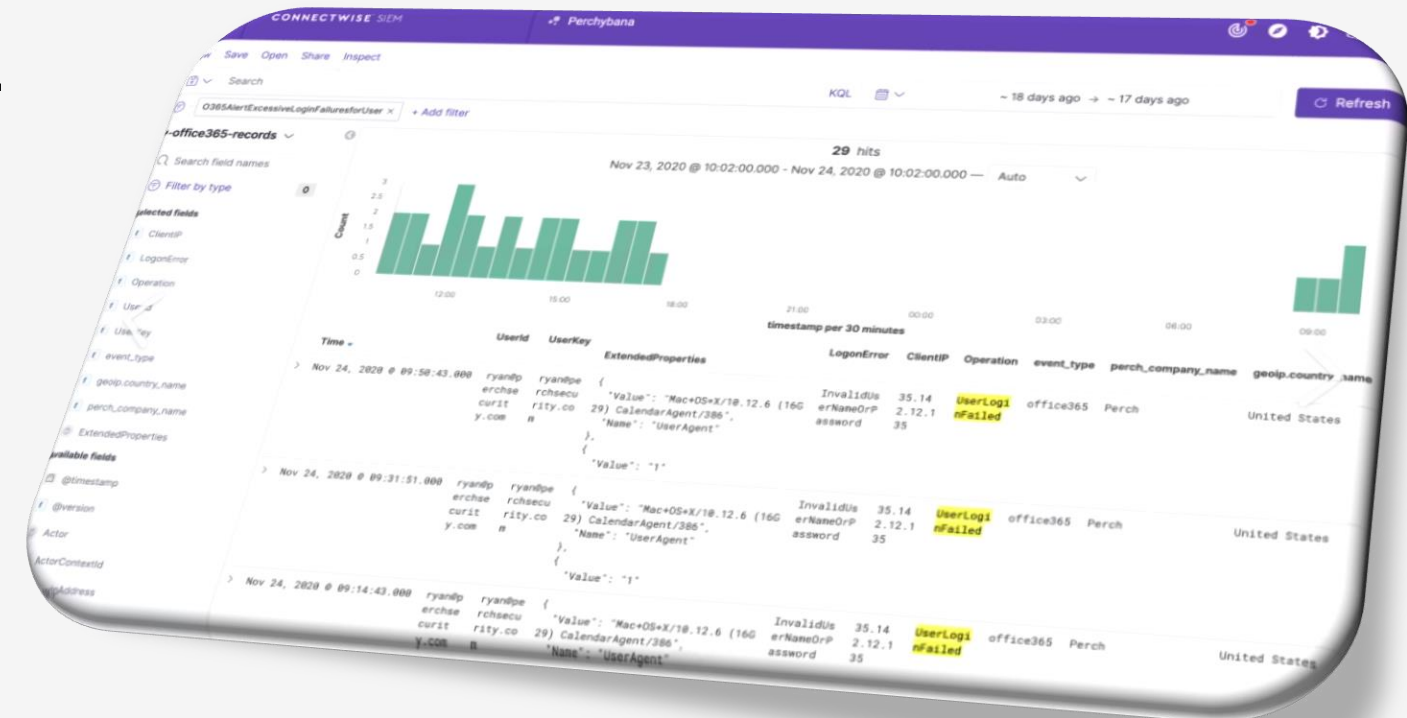
24/7 Security Operation Center

Continuous monitoring of your infrastructure to detect, respond to, and mitigate threats in real time.

02

SIEM (Security Information Even Management)

Centralized log management and real-time analysis of security events to quickly identify suspicious activity across networks and systems.



Managed Vulnerability Management

03

Regular Vulnerability Scanning

Scheduled scans of the entire network to detect weak points or misconfigurations in systems, software and devices.

04

Patch Management

Ensuring that operating systems are up-to-date with the latest patches to eliminate known vulnerabilities.

05

Internal and External Penetration Testing

Simulating real-world attacks to identify and fix weaknesses before hackers can exploit them.

Project Based

Managed Endpoint Detection & Response

06

Managed Endpoint Detection & Response

Advanced security for all endpoints (laptops, desktops, mobile devices) that goes beyond traditional antivirus to detect sophisticated threats like fileless malware and ransomware.

Automated Threat Containment

Quick isolation of compromised endpoints to prevent spread of threats across the network.



Identity and Access Management (IAM)

07

Multi-Factor (MFA)

Implementing MFA to add extra layer of security by requiring users to verify their identity beyond just a password.

08

Single Sign-on (SSO)

Secure, centralized access management that allows users to log into with one set of credentials while maintaining strong security controls.

09

Privileged Access Management (PAM)

Ensuring that only authorized personnel have access to sensitive systems, with strict monitoring of privileged accounts.

Project Based

Managed Network Security

10

Firewall Management

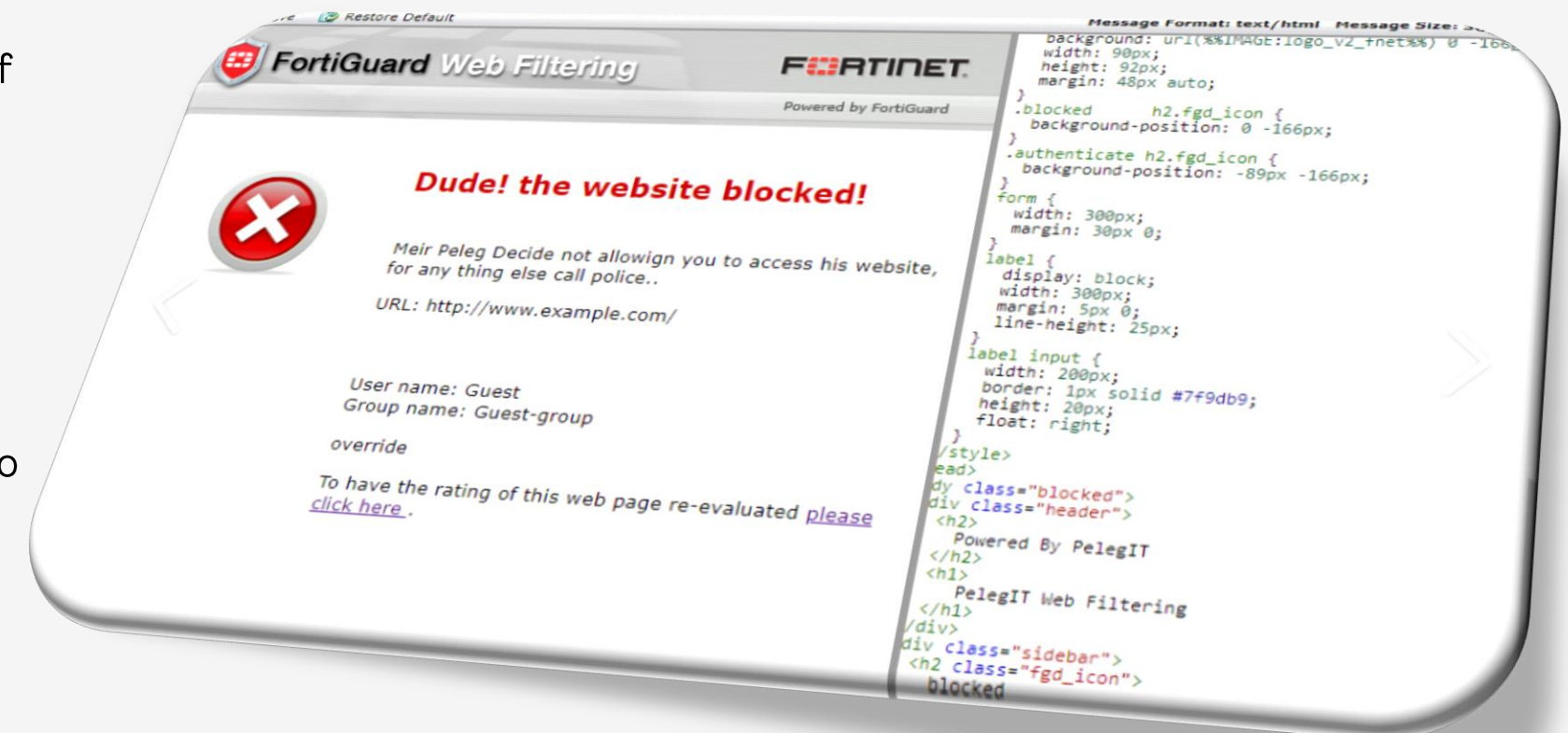
Advanced configuration, monitoring, and updating of firewalls to defend the network perimeter.

Intrusion Detection and Prevention (IDPS)

Continuous monitoring of network traffic for suspicious activities or instructions and taking action to block potential attacks.

Web Filtering

Preventing users from accessing malicious or inappropriate websites that could introduce risk to the network.



Network-As-A-Service (NaaS)

Price Starts at \$350 Per Month

SMALL Business

Under 50 Users
1 Gbps Inspected Internet

Includes:

- 2 ISP connections
- 10 Firewall Rules
- 3 Security Profiles
- No IPSEC VPN's
- 1 SSL User VPN Profile
- Single LAN Interface
- No DMZ
- No Guest Interface
- Configuration Conversion

Price Starts at \$450 Per Month

MED Business

Under 100 Users
2.2 Gbps Inspected Internet

Includes:

- 2 ISP connections
- 50 Firewall Rules
- 3 Security Profiles
- 1 IPSEC VPN's
- 1 SSL User VPN Profile
- Single LAN Interface
- No DMZ
- 1 Guest Interface
- Configuration Conversion

Price Starts at \$550 Per Month

LARGE Business

Under 250 Users
3.5 Gbps Inspected Internet

Includes:

- 2 ISP connections
- 200 Firewall Rules
- 5 Security Profiles
- 2 IPSEC VPN's
- 1 SSL User VPN Profile
- Three LAN Interface
- 1 DMZ
- 1 Guest Interface
- Configuration Conversion

Monthly price includes installation and onboarding, 24x7 monitoring, patching, configuration backups, and SOCaaS (24x7 Cloud Based Managed Log Monitoring, Incident Triage and SOC escalation service). Unlimited support tickets.

Managed Backup & Recovery

11

Backup & Disaster Recovery

Secure, automated backups and disaster recovery plans that allow for quick restoration of data after an indicate or outage.

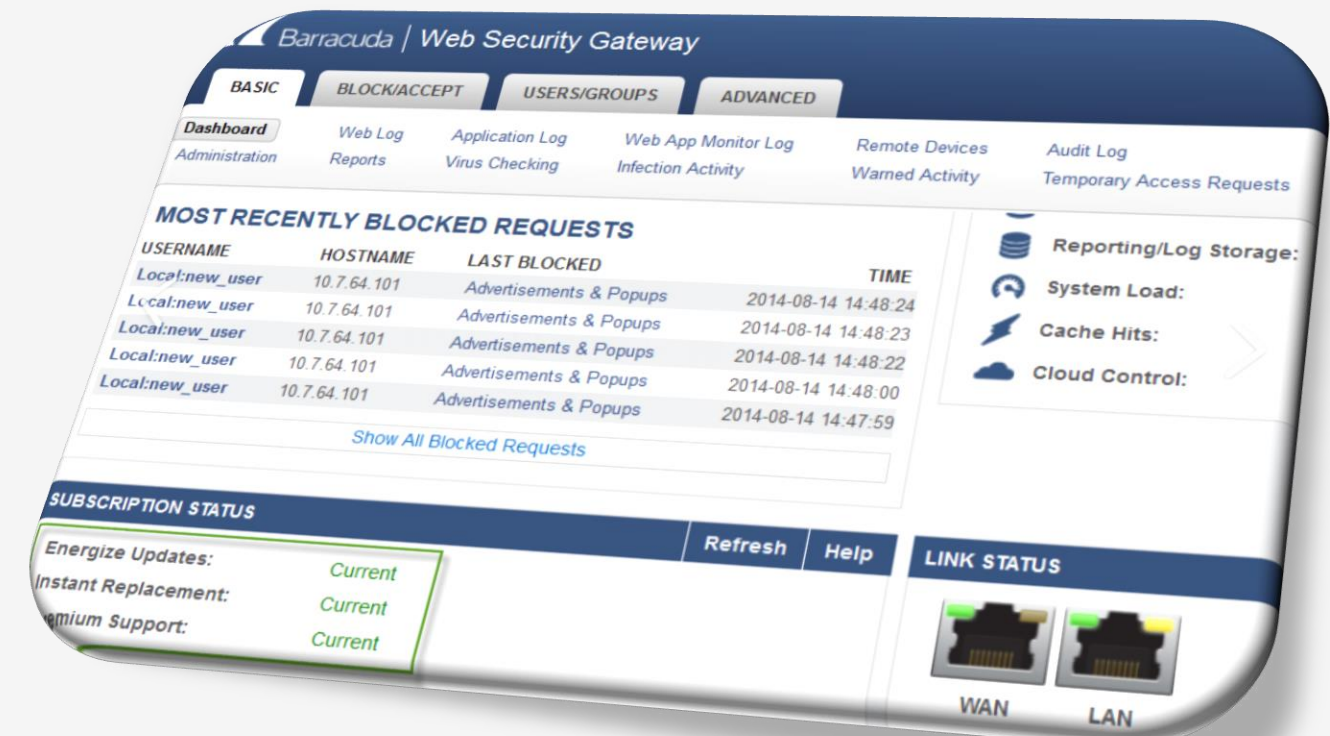


Email and Web Security

12

Email Filtering & Anti-Phishing Protection

Blocking malicious emails, phishing attempts, and spam before they reach employees inboxes.



Compliance & Risk Management

13

Security Audits & Risk Assessments

Regular audits to evaluate the strength of current security measures, identify risks, and provide recommendations for improvement.

14

Security Awareness Training

Providing ongoing education and simulations for employees to help them recognize phishing attacks, social engineering, and other threats.



October is Security Awareness Month!

Risk Assessment Report



Thank you for taking the time to participate in this risk assessment process. The goal of this assessment is to identify your security strengths and weaknesses, and to provide advice as to the improvements you should be considering relative to your security posture.

The assessment and your results are aligned to the National Institute of Standards and Technology, Cybersecurity Framework v1.1, (NIST CSF), considered to be a best practice for firms such as yours.

The assessment spanned the five core areas of the framework as detailed below, and this report will show you results against the framework, as well as how your business aligns to other firms with respect to size, location, and industry.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
<ul style="list-style-type: none">• ASSET MANAGEMENT• BUSINESS ENVIRONMENT• GOVERNANCE• RISK ASSESSMENT• RISK MANAGEMENT STRATEGY• SUPPLY CHAIN RISK MANAGEMENT	<ul style="list-style-type: none">• ACCESS CONTROL• AWARENESS & TRAINING• DATA SECURITY• INFO PROTECTION PROCESS & PROCEDURES• MAINTENANCE• PROTECTIVE TECHNOLOGY	<ul style="list-style-type: none">• ANOMALIES & EVENTS• SECURITY CONTINUOUS MONITORING• DETECTION PROCESSES	<ul style="list-style-type: none">• RESPONSE PLANNING• COMMUNICATIONS• ANALYSIS• MITIGATION• IMPROVEMENTS	<ul style="list-style-type: none">• RECOVERY PLANNING• IMPROVEMENTS• COMMUNICATIONS

For your reference we have provided a link to the NIST Cybersecurity Framework and encourage you to download the document and become more familiar with the valuable information that can help you in your journey to better secure your business.

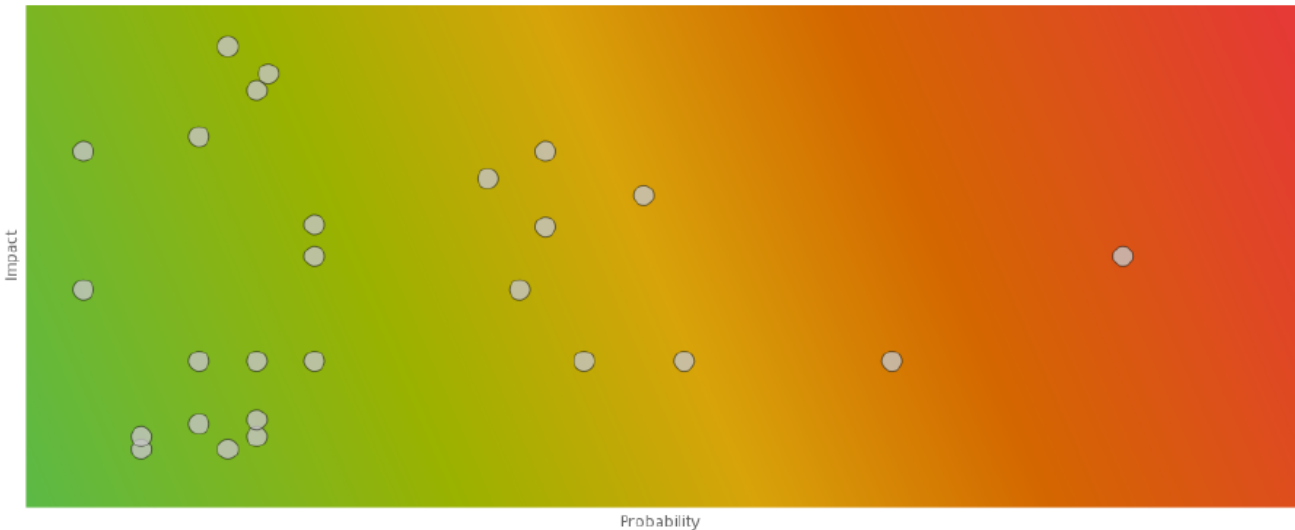
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>



OVERALL RISK ASSESSMENT


Your overall risk rating is **LOW**

Congratulations! Your overall risk determined from the assessment conveys a diligence on your part to ensure you are doing what is needed to maintain the security of your organization.



TOP RISK AREAS

- Critical** PR.AT-1 - All users are informed and trained
- High** ID.RA-1 - Asset vulnerabilities are identified and documented
- High** ID.RA-2 - Threat and vulnerability information is received from information sharing forums and sources
- Medium** PR.PT-3 - The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
- Medium** RS.RP-1 - Response plan is executed during or after an event



TOP RISK AREA RECOMMENDATIONS

PR.AT-1: All users are informed and trained

Critical

Q: Do you require Information Security training for your employees?

A: No

Importance:
It is essential to your business to ensure your employees are trained on the constantly changing security threats and how to avoid these threats.

Remediation Steps:
There are several on-line security awareness training companies. Make it a priority to sign your employees up for annual security awareness training.

ID.RA-1: Asset vulnerabilities are identified and documented

High

Q: Does your organization have an internal process for assessing risk?

A: No


Importance:
Along with having security policies, a risk assessment is the most fundamental element to protecting your vital business assets. By not having one performed you are essentially blind to the risks and severity of the risks that can impact your business.

Remediation Steps:
Create a policy for performing periodic risk assessments, and work with a skilled professional to schedule an assessment.

ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources

High

Q: Do you receive threat intelligence information from sharing sources such as ISACs?



PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

Medium

Q: How long before your computer screen is set to lock when not in use anytime you're away from your computer?

A: 15 minutes

Importance:
It's good that you have configured your computers to lock automatically 15 minutes after non-use, best practice is to lock screens after 5 minutes of non-use.


Remediation Steps:
Implement an auto-lock feature for a set period of time, no more than 15 minutes, and get into the practice of locking it manually consistent with the operating system that you are using.

Q: Do you allow the use of USB ports?

A: Yes

Importance:
Using USB ports can be useful for transferring files, doing backups and other routine operational procedures; however, they are an easy way for employees to copy and share confidential data that you would not want to be shared. They also pose a risk of introducing malware into your environment.

Remediation Steps:
Update or create a policy regarding restrictions of USB for business use. If you must allow them then you should have control over the inventory and not allow employees to use their own USB devices.



RS.RP-1: Response plan is executed during or after an event

Medium

Q: Do you have incident response processes and procedures in place which are being maintained on a regular basis?

A: No

Importance:
It is critical for your business to be able to respond to and recover from a security event and you don't have a plan to do so.

Remediation Steps:
Create a business continuity and disaster recovery plan for your business. Work with a security consulting firm if you need assistance creating these plans.

Q: Are you planning on developing incident response processes and procedures?

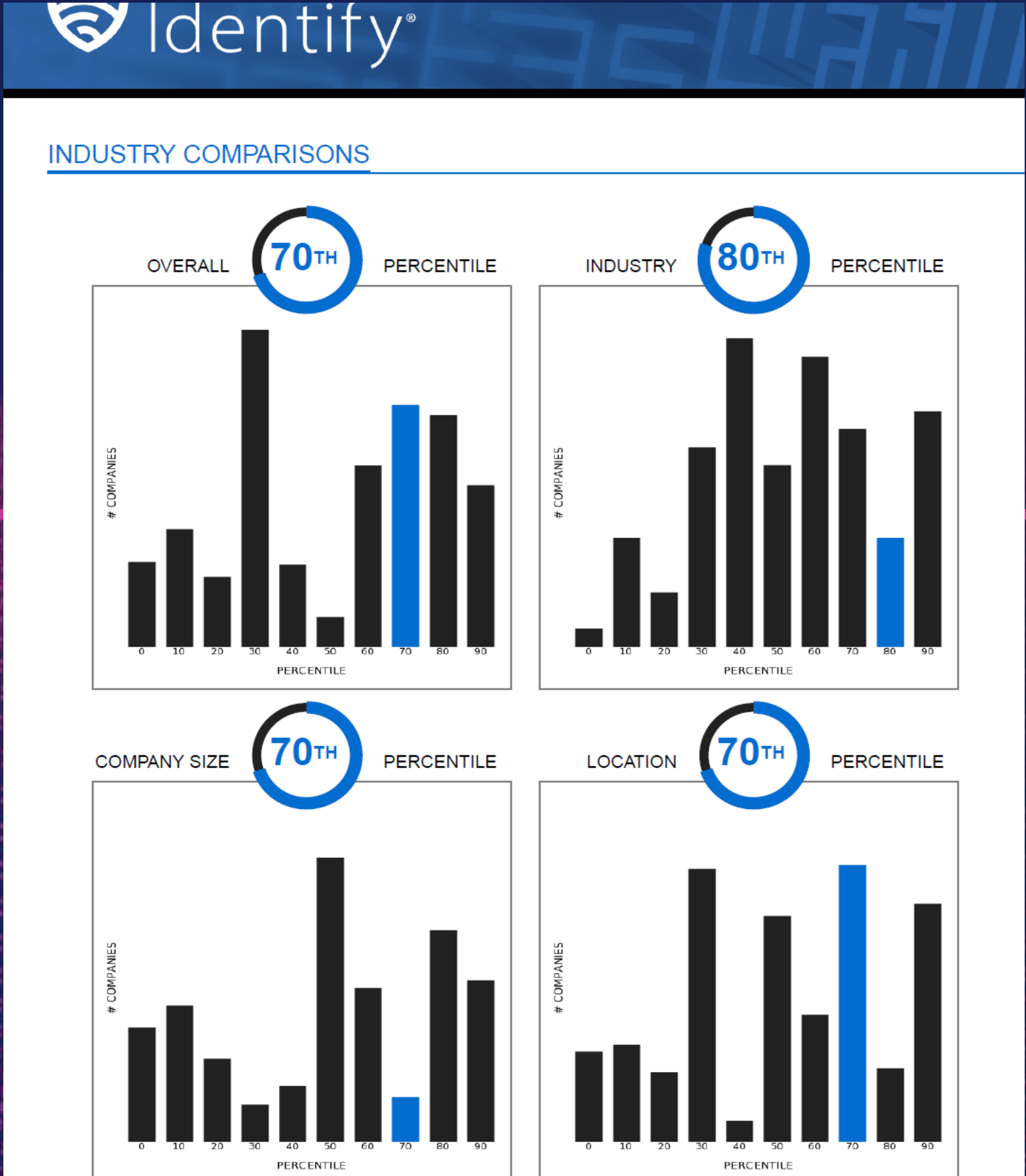
A: Yes

Q: What is the time frame you are looking at to develop incident response processes and procedures?

A: Within a Year

Importance:
Having response processes and procedures to ensure your business can continue to run after a recovery is needed is critical.

Remediation Steps:
You should consider moving your plan to create recovery processes and procedures up in priority and complete within the next six months. There are professional services available who can assist you with this process.



Mobile Device Management (MDM)

15

Mobile Security

Implementing and managing security policies for mobile devices used by employees, ensuring protection against unauthorized access, data leakage, and mobile malware.

Remote Wipe Capabilities

The ability to remotely lock or erase data from lost or stolen mobile devices to prevent unauthorized access.



Professional Services

Incident Response (IR) and Threat Remediation:

Rapid response to security incidents, including malware infections, ransomware attacks, and data breaches, with well-defined recovery procedures.

Proactive Threat Hunting

Actively searching for potential vulnerabilities or emerging threats within your environment, using threat intelligence feeds, advanced analytics and expert analysis.

Zero Trust Architecture

Implementing a “never trust”, always verify” approach by ensuring no device or user has access without authentication and validation.

Cloud Security Management

Ensuring secure configuration and monitoring of public, private and hybrid cloud environments.

Cloud Access Security Broker (CASB)

Securing data and applications that are hosted in the cloud by providing visibility, compliance enforcement, and protection against cloud-native threats.

If you sign up for Managed Services, you are entitled to 20% service discount security related projects.

Business Case Outsourced Security



● Cost Savings

Hiring and retaining top-tier security professionals in-house can be expensive. By using our MSP, you avoid the costs of recruitment, training and full-time salaries.

● Predictable Budgeting

Our services come with fixed monthly fees, giving you predictable costs and preventing the need for unexpected budget allocations when security issues arise.

● Avoid Downtime

Cyber-attacks can result in significant downtime. With a dedicated MSP managing your security, the risk of downtime decreases dramatically, saving you money and maintaining operational efficiency.

Managed Service Offerings

FLEXIBLE WAYS TO BUY

Basic

- Centralized Management Portal
- Proactive alerts
- Network monitoring
- Patching
- Webroot secure anywhere
- ScreenConnect
- System Tray Communicator

Essentials

- Centralized Management Portal
- Proactive alerts
- Network monitoring
- Patching
- Webroot secure anywhere
- ScreenConnect
- System Tray Communicator
- Quarterly Core Networking Review and Updates

Hassle Free

- Centralized Management Portal
- Proactive alerts
- Network monitoring
- Patching
- Webroot secure anywhere
- ScreenConnect
- System Tray Communicator
- Quarterly Core Networking Review and Updates
- Unlimited reactive support
- Predictive support costs
- End users access to help desk engineers

Enterprise

- Centralized Management Portal
- Proactive alerts
- Network monitoring
- Patching
- Webroot secure anywhere
- ScreenConnect
- System Tray Communicator
- Quarterly Core Networking Review and Updates
- Unlimited reactive support
- Predictive support costs
- End users access to help desk engineers
- Virtual CIO

Focus on Innovation, Not Firefighting

Your IT Team's core mission

Driving business innovation, improving operations and delivering value.

Let IntegraONE handle the heavy lifting of security so that you can focus on what matters the most.

OUR CLIENTS' SUCCESS IS OUR SUCCESS

"They were very attentive to our needs throughout the entire process."

Good Shepard Rehabilitation

"...Extremely impressed with their ability to understand and respond to our IT needs."

Lebanon Federal Credit Union

"I never feel like I am being sold products or services."

Sunstone Consulting

"...Fantastic partner to us in everything we've done." Benco Dental

OUR CLIENTS' SUCCESS IS OUR SUCCESS

"...We don't want to use anybody else because they've always given such great service."

Northampton Community College

"...Increase in productivity, reliability, and the overall health of our IT environment."

Lebanon Federal Credit Union

"We have built a great relationship."

Sunstone Consulting

"We look at IntegraONE as part of our team." Spooky Nook Sports

A tradition of success & support

170+

customers

5000+

desktops

500+

servers

1500+

network devices

5X

winner of CRN
MSP 500 List

1990

year IntegraONE
was founded

2007

year MSP was
first offered

**It's all in the
numbers**

5 local offices:

Allentown, PA • Philadelphia, PA • Harrisburg, PA • Wilks-Barre, PA • Pittsburgh, PA

Why IntegraONE?

Partnerships, Not Replacement:

Unlike other MSPs that may try to take over your IT Operations, we specialize in co-managed IT services. We enhance your existing IT team by adding specialized expertise.

Tailored Security Solutions:

We don't believe in one-size-fits-all. We offer customized security solutions that fit your business's specific needs, whether you're a small business or large enterprise.

We want to be your trusted partner

Future Hyperautomation Strategy

Driving Efficiency through Automation

Hyperautomation uses advanced AI and machine learning to predict and resolve potential issues before they impact your business.

By adopting a hyperautomation strategy, IntegraONE is committed to delivering faster, more reliable and cost-effective services. It will allow your business to operate more smoothly, reduce IT-related disruptions, and grow without the typical IT bottlenecks. With a more automated and intelligent system behind you, your business is free to focus on what really matters – your customers and growth!

Questions & Answers

Contact Us



www.integraone.com



djuhasz@integraone.com



484-223-3480 x1215



7248 Tilghman Street
Allentown, PA 18106

