

MSBO Technology Committee and VDA Labs



Cybersecurity : **Where do I begin?**

VDA LABS

Ryan Carter, CNA, CNLM
rcarter@vдалabs.com



Technical Account Manager / PSE w/VDA Labs

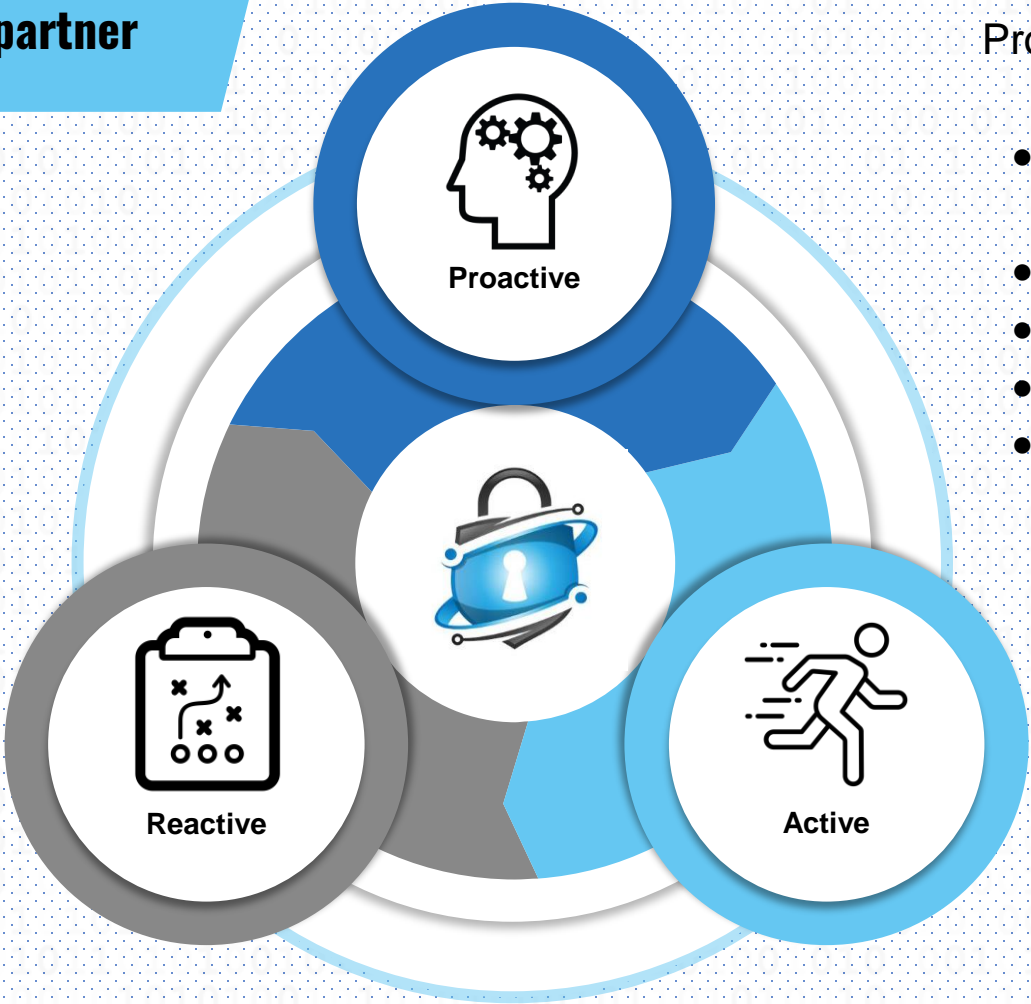
- Over 25 years experience in the IT field, started in 1990.
- Certificate in Non-Profit Leadership and Management thru MSU, ITIL v3 Certified, Scrum Certified, Certified Novell Admin.
- Held Executive Director level positions in Non-profit, Manufacturing, Insurance, State Government and IT Consulting sectors.
- Owned and operated an IT consulting practice since 1998.

Focus knowledge areas at VDA:

- Penetration testing “Red Team” attacks and Network Vulnerability assessments.
- Firewall security solutions - Palo Alto and Fortinet.
- 2 Factor authentication solutions – Okta & DUO
- EDR products - Sentinel One, Palo Alto Cortex XDR
- SIEM / SOC / SOAR platforms – VDA Vigilance, GrayLog, ElkStack, LogRhythm.
- GRC compliance frameworks - NIST, CMMC, ISO27001, SOC2, PCI, HIPAA.
- End user security awareness training platforms – VDA Aware, KnowBe4

VDA Labs Client Engagement

Your end-to-end cybersecurity partner



Reactive

- Incident Response Team
- Forensic Investigation
- Threat Hunting
- IR Planning & Roadmap
- Business Continuity
- Incident Response Events
 - Table Top
 - Active Hacking
 - Red Team Exercises
 - Simulated Disaster Recovery

Proactive

- Security Program Development
- Compliance Consulting
- Adversarial Testing
- Application Security
- Product Evaluation & Resale

Active

- VDA Vigilance
 - Managed SIEM
 - SOC-as-a-Service
 - Managed Detection & Response
 - Comprehensive Threat Intelligence
 - 24x7 Monitoring

**Kent
ISD** 

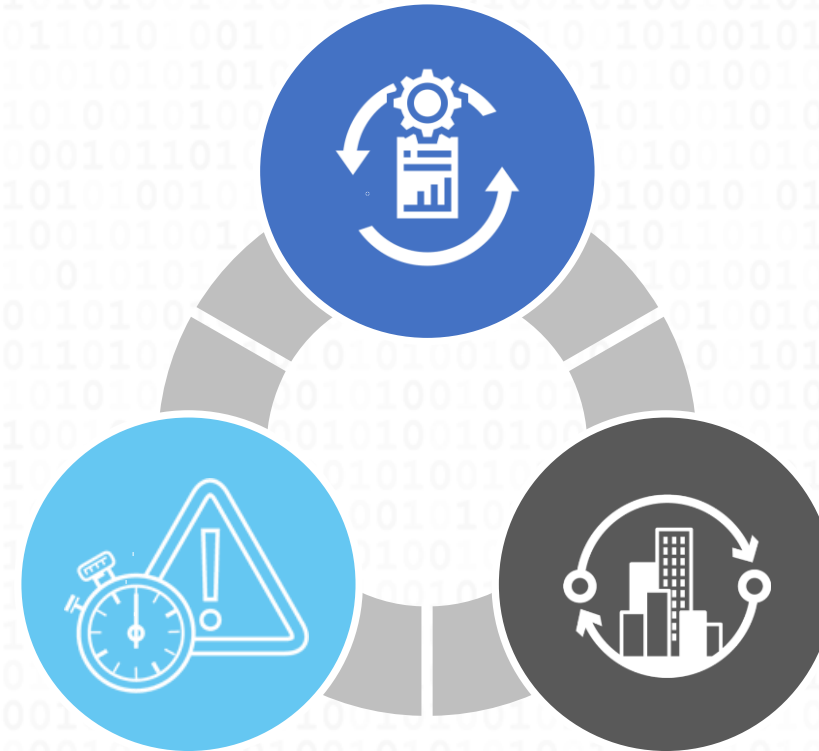
&

VDA LABS

Kent ISD - Contingency Planning

Why We're Here

- Preparation is the key to mitigating risk and/or crisis aversion
- Standardization of plans across districts with tailored practices towards educational institutions
- Keep operations running in the event of several common scenarios



Disaster Recovery

Patterns the recovery process back to normalcy. Focuses on system and data availability.



Incident Response

Documentation of how your district handles an incident from the start.

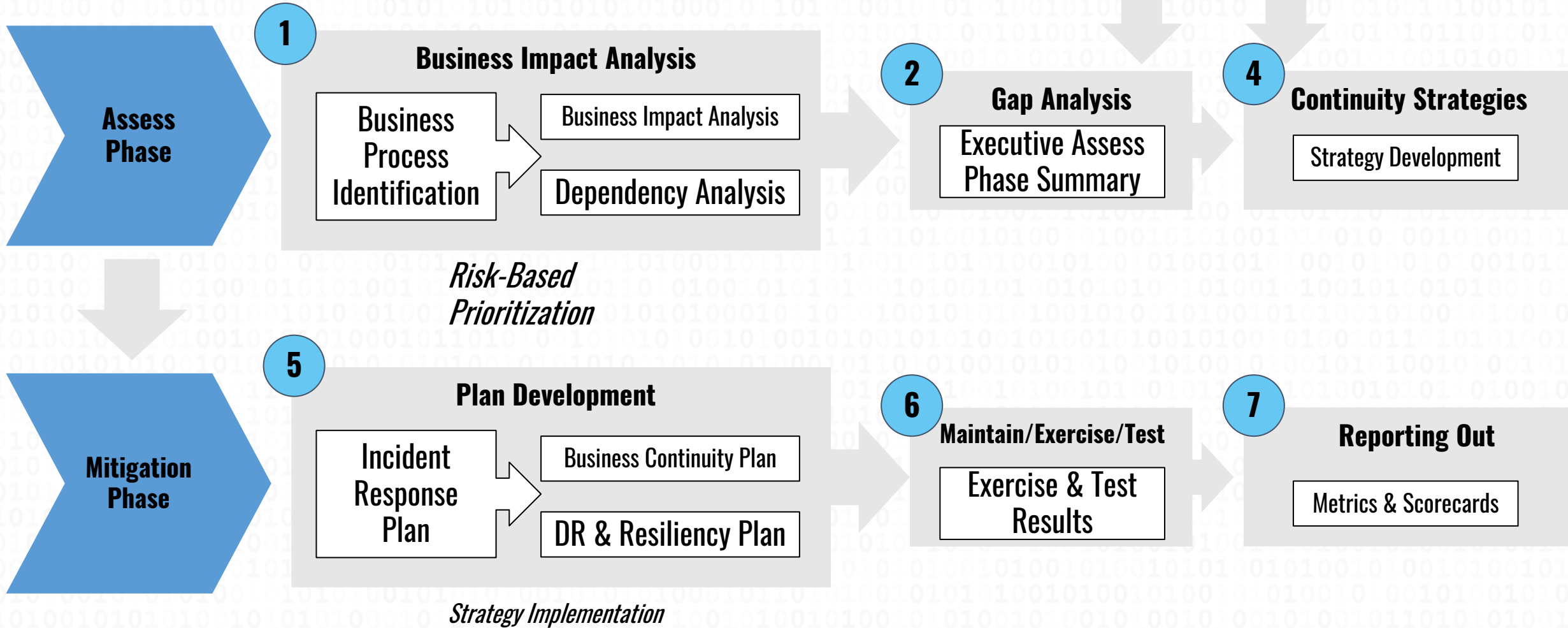


Business Continuity

Keeps your organization running during the lifecycle of an incident.

Kent ISD - Contingency Planning

Project Workflow



Kent ISD - Contingency Planning

BIA Homework Assignment

- Develop a Business Impact Analysis document based on your environment
- Define Critical People, Systems, Applications and Locations
- Define the critically of the systems outages
- Define your RPO/RTO and Maximum Tolerable Downtime

[School District]: District or School Impact Assessment

Classification: Confidential

People

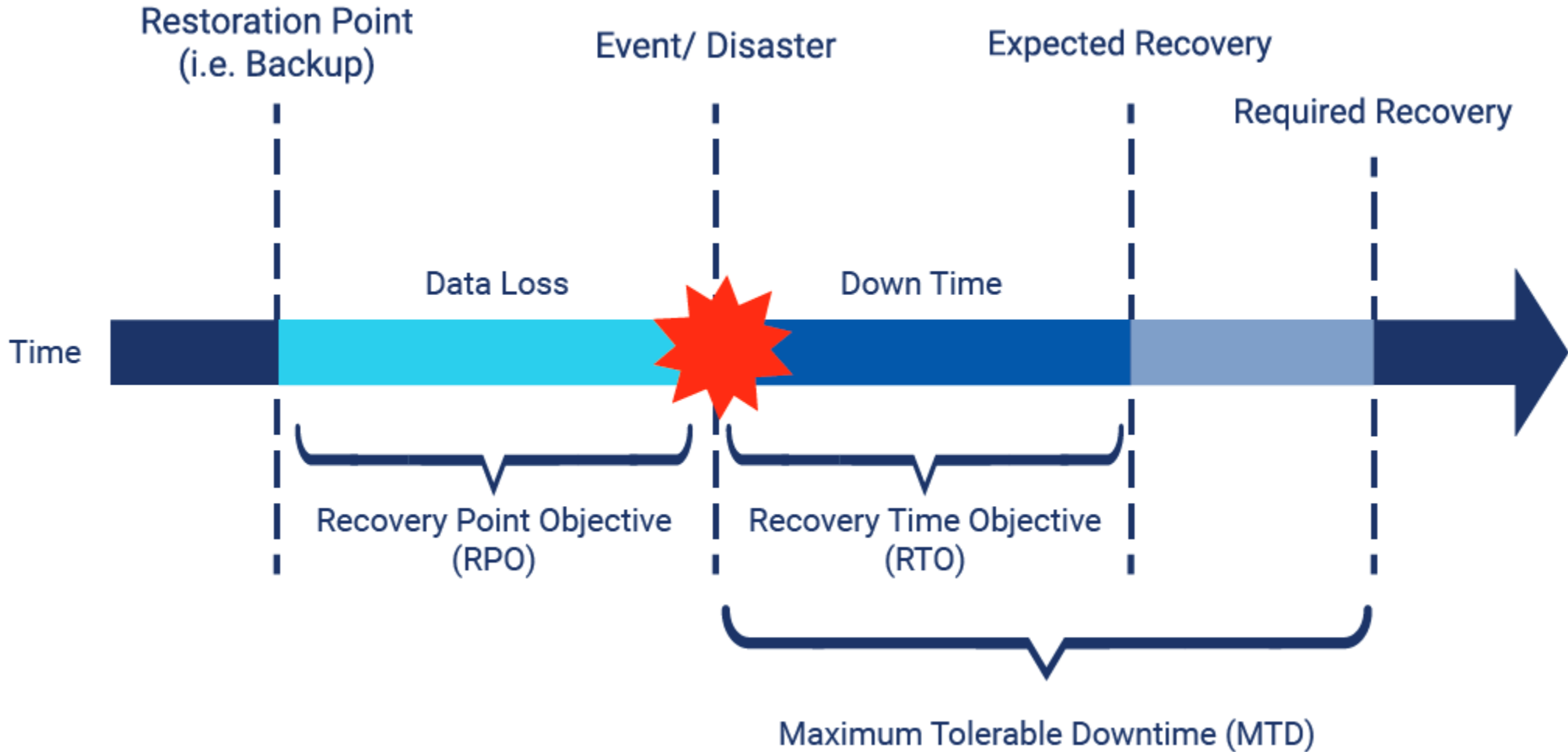
Department / Function	Department / Function Priority	Head of Department / Function	Number of Full Time Staff	Number of Volunteers	Number of Part Time Staff	Number of Contractors	Work From Location	Impact Over	
								0 to 1 days	2 to 4 days
IT	High							Low	Medium
Operations	High							Low	Medium
Software Development	Medium							Low	Medium
HR	Medium							Low	Medium
Finance	Low							Low	Medium
Marketing	Low							Low	Medium

Internal Systems

What it does	What it is called	Who Uses It	Acceptable time to restore (RTO - Recovery Time Objective)	Acceptable Point of Recovery (RPO - Recovery Point Objective)	Maximum Tolerable Period of Disruption (MTPoD)	Impact Over time			
						0 to 1 days	2 to 4 days	5 to 10 days	> 10 days
Accounting System						Low	Medium	High	Catastrophic
HR System						Low	Medium	High	Catastrophic
Email						Low	Medium	High	Catastrophic
File Storage						Low	Medium	High	Catastrophic
Company Website						Low	Medium	High	Catastrophic
Web Hosting						Low	Medium	High	Catastrophic
Source Code Management						Low	Medium	High	Catastrophic
CRM						Low	Medium	High	Catastrophic

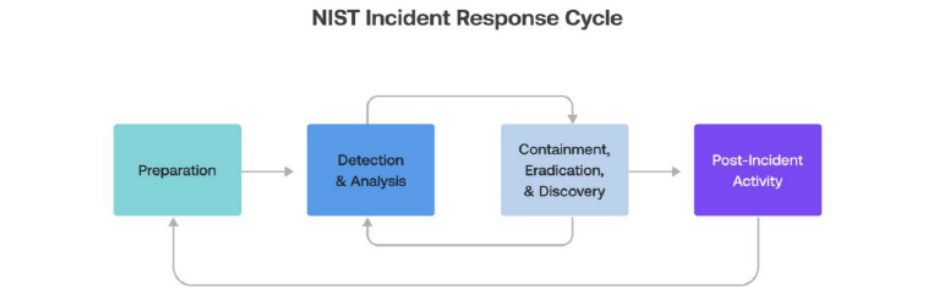
Kent ISD - Contingency Planning

What Does RPO & RTO Mean?





<p>Initial Disaster Recovery Workshop</p>	<p>Two working sessions will be made available between workshops for a duration of two hours per working session. These will be optional sessions for districts to follow up on any items covered in the initial workshop.</p>	<p>Follow-up Disaster Recovery Workshop</p>
<p>Sample areas and topics of discussion as they relate to distributed template</p> <ul style="list-style-type: none"> ● Insurance Compliance ● Identify Critical Operations ● Evaluate Possible DR Scenarios ● Develop a Communication Plan ● Developing a Data Backup and Recovery Plan ● Testing Regime 		<p>Topics of discussion and workshop structure will include, but are not limited to the following:</p> <ul style="list-style-type: none"> ● Peer Review Process ● Testing Effectiveness (Applicability & Scenarios) ● Testing Cadence ● Plan Maintenance ● Plan Adaptability and Approval Processes



<p>Initial Incident Response Workshop</p>	<p>Two working sessions will be made available between workshops for a duration of two hours per working session. These will be optional sessions for districts to follow up on any items covered in the initial workshop.</p>	<p>Follow-up Incident Response Workshop</p>
<p>Sample areas and topics of discussion as they relate to distributed template</p> <ul style="list-style-type: none"> ● Insurance Compliance ● Preparation ● Detection ● Analysis ● Containment ● Recovery ● User Response 		<p>Topics of discussion and workshop structure will include, but are not limited to the following:</p> <ul style="list-style-type: none"> ● Peer Review Process ● Testing Effectiveness (Applicability & Scenarios) ● Testing Cadence ● Plan Maintenance ● Plan Adaptability and Approval Processes
<p>Additional topics of discussion will include, but are not limited to the following:</p> <ul style="list-style-type: none"> ● Reporting of cyber incidents <ul style="list-style-type: none"> ○ Identification of affected systems ○ Detecting affected accounts ○ Detecting affected data ○ Additional possible areas of compromise 		



<p>Initial Business Continuity Workshop</p>	<p>Two working sessions will be made available between workshops for a duration of two hours per working session. These will be optional sessions for districts to follow up on any items covered in the initial workshop.</p>	<p>Follow-up Business Continuity Workshop</p>
<p>Sample areas and topics of discussion as they relate to distributed template</p> <ul style="list-style-type: none"> ● Insurance Compliance ● Business Impact Framework ● Outage Maps & Impacts ● Estimating Downtime ● Triaging Recovery Priorities ● Assigning Metrics & Cost Assessment ● Communication Processes 		<p>Topics of discussion and workshop structure will include, but are not limited to the following:</p> <ul style="list-style-type: none"> ● Peer Review Process ● Testing Effectiveness (Applicability & Scenarios) ● Testing Cadence ● Plan Maintenance ● Plan Adaptability and Approval Processes

Services and solutions we recommend to reduce the attack surface:

- Implement MFA
- Update traditional AV to EDR
- Implement SIEM/SOC/SOAR
- Implement DLP
- Implement PAM
- Implement IAM
- Regular Pen testing
- Internal vulnerability management
- Security GAP assessments following a framework
- Creation of IR, DR and BC plans following NIST

Baseline / lower cost initial engagements:

CIS top 18 security controls assessment – aligned to NIST 800-171 / CSF

AD/Azure security review – Hardening and best practices

AWS container / workload security assessment – Container security / risk score improvement

O365 security audit – Hardening, attack surface reduction, secure score improvement

Vulnerability management – quarterly internal security scans


EUT and quarterly rotating phishing assessments – Implement a district wide user training platform


Software / Hardware asset inventory scan – Utility used to scan the IT environment to report assets


MSSP offerings: Helping to remove the workload off small or overloaded IT teams


MSSP Offerings


VDA Labs is invested in bolstering security defenses against the constantly growing threat landscape in today's interconnected workplace. These offerings are structured to comply with today's typical cybersecurity insurance requirements, as well as best practice solutions to combat threat actors effectively, maximize uptime, and minimize the possibility of a breach scenario.

Cybersecurity Awareness Program
Web-based application designed to train personnel on the pressing need to be cyber vigilant. Includes 6 Modules & semi-annual phishing simulation tests (2 per year). 


Email Security
Filters/scans incoming emails for malicious attachments and/or links. Includes Secure Email Gateway, Targeted Threat Protection, and Internal Email Protect. 


DNS Security
A protective DNS service that prevents access to domains known to be malicious. Cloud-delivered network security and threat intelligence that protects any device, anywhere. 


Data Backup
Data backups are disconnected and inaccessible through the organization's network. Administered in a secure cloud environment. Includes regularly tested restoration & recovery. 


Patch Management
Automate vulnerability identification and remediation with patch management. Includes service to install critical software security patches within 30 days. 


MSSP Offerings


Endpoint Detection & Response
Next-Generation Antivirus Static AI & Behavioral AI Prevention. Embedded AI Threat Intel & Threat Indicators. Recovery with 1-Click Remediation & Rollback. VDA Labs MDR included. 

Password Management
Password manager that stores encrypted passwords online. Saves your passwords and gives you secure access from every computer and mobile device. 


VDA Vigilance - SIEM /MDR - Monitoring
Managed log aggregation software to correlate security information and events to centrally managed platform with user and entity behavior analytics (UEBA). VDA Labs MDR included. 


Mobile Device Management
Protect every endpoint with flexible device categorization, intelligent auto-deployment of configurations, and auto-mapping of identity to devices. 


Vulnerability Management
Identification, handling, and reporting on security vulnerabilities in systems and the software that runs on them. Service provided quarterly by VDA Labs. 


Incident Response Plan
VDA Labs will work to provide a set of tools and procedures that your security team can use to identify, eliminate, and recover from cybersecurity threats (including ransomware events). 

MSSP Offerings

Active Threat Hunting
Huntress enables you to find and stop hidden threats that sneak past preventive security tools. This platform helps IT service providers protect themselves from persistent footholds, ransomware, and other attacks. 

Multi-Factor Authentication (2FA/MFA)
Multi-factor authentication (MFA) is used to protect against hackers by ensuring that digital users are who they say they are. Not having MFA is one of the most common means of account compromise. 

Web Application Firewalls (WAF)
Web Application Firewalls (WAF) helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. Protects against cross-site scripting (XSS), SQL injection, cookie poisoning, and more. 

vCISO
A dedicated security practitioner who uses the culmination of their years of cybersecurity & industry experience to help organizations with developing and managing the implementation of the organization's information security program. 

Value with Purpose	Simple & Predictable Pricing	Fast Deployment
❖ Meets compliance requirements	❖ Flexible Billing	❖ Solutions deployed in 30 days or less
❖ Proposed solutions managed by VDA Labs	❖ Priced by user, endpoint, or site (depending on solution)	❖ Licensing issued within 48 hours
❖ Modern tools & technologies for best-of-breed protection	❖ Multi-year options available	❖ Visibility gained immediately after onboarding



VDA@LABS

Ryan Carter, CNA, CNLM

rcarter@vдалabs.com

QUESTIONS?

