RAZOR TECHNOLOGY

Collaborative Protection: Strengthen Cyber Security with Razor Technology "Secure Office Platform"

Ryan Rosenkaimer – VP, Managed Services and Security

About Me

- Over 20 Years working in tech.
- Drives overall technical direction and service offerings for Razor.
- Passionate about delivering customer success with technology.
- Helping businesses transform around compliance and governance as a virtual CTO/CIO/CISO.

  - Philly native.
  - I have an extensive LEGO collection.
  - I will never turn down a soft pretzel.

Ryan Rosenkaimer

Vice President, Managed Services and Security

Who is Razor Technology?

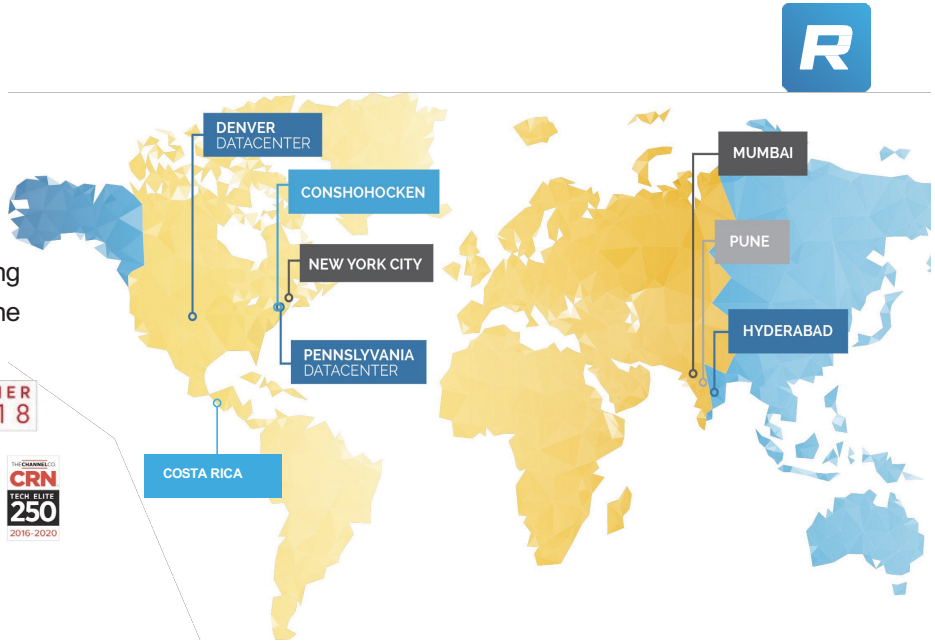
Our Team

Connect with the razor technology team for an insider's look at the tools that are reshaping business and gain invaluable insights on how digital transformation can give your brand the edge it needs to compete in the modern marketplace.

256 + CERTIFICATIONS

ALL FORMER END-USERS

EXPERTS IN THE TOP 20 TECH VENDORS



Delivering Digital Confidence

Razor Technology's tailored IT solutions examine the needs of individual businesses and the people behind them, creating infrastructures that minimize downtime and reduce friction in all processes.

RAZOR TECHNOLOGY
Delivering Digital Confidence.
MODERN HELPDESK

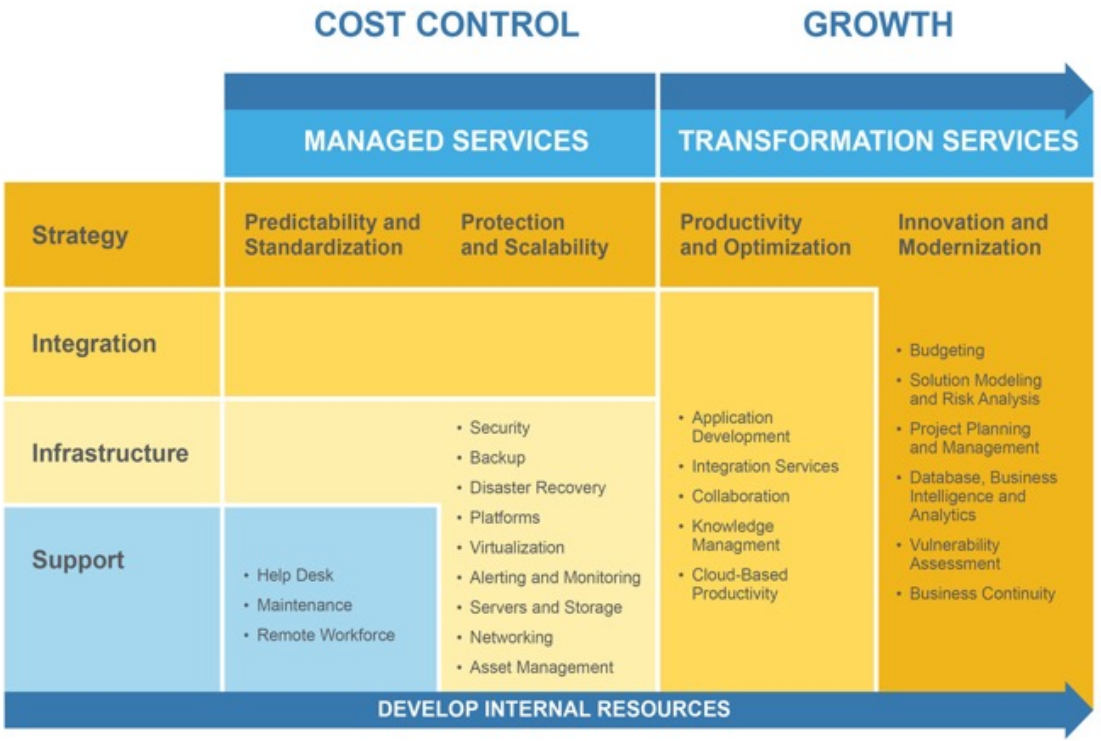
The Razor Value Model

Our model is not designed to displace internal resources. It is designed to help them develop the specialized skillsets that have the greatest future value to themselves, your organization, and most importantly, your customers.

As your organization grows, our model allows you to scale without adding maintenance and support resources. IT staff leave for better opportunities and lesser aggravation. Our model is designed to help you provide those better opportunities for them within your organization and relieve them of the burdens that cause them the greatest frustrations.

Our value model serves two primary priorities for our clients.

Managed Services for the Modern Workplace



GVA SECURE OFFICE

POWERED BY RAZOR TECHNOLOGY

Technology Management & Support:

- **Endpoints** - Desktops & Mobile Devices
- **Network Devices** - Firewalls, Switches and WAPs
- Software Patch Management – Windows updates for workstations
- Virus, Anti-Spam and Web Filter Software
- Asset Management
- Monitoring of Desktop and Network Infrastructure
- Remote Support Service Desk – 24 x 7 x 365
- Microsoft Application Support

Increased Security:

- Microsoft Authenticator – MFA – Single Sign-On (SSO)
- Data Loss Protection Policy Controls

Microsoft Office 365 E5

- Office 365 Advanced Threat Protection (ATP)

  ATP Safe Links - protects the organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents.

  ATP Safe Attachments - this feature checks to see if email attachments are malicious, and then takes action to protect your organization.

Managed Detection and Response

- Monitors endpoints on and off the network around the clock with a 24 x 7 x 365 Global Security Operations Center.
- Protects your endpoints anywhere users and data reside–across cloud, mobile, virtual, and physical environments.
- Accelerates forensic investigation, acting as a "black box" flight recorder that continuously records, centralizes, and retains vital endpoint activity.
- Catches what prevention misses with proprietary machine learning layered with attack pattern and behavioral analytics.
- Locks down and isolates threat actors on your behalf preventing lateral spread and potential business disruption.

Microsoft 365 E5 includes

Word, Excel, PowerPoint, Outlook, OneNote, SharePoint, OneDrive, Microsoft Teams, Power BI Pro, Windows, Microsoft Endpoint Manager

Additional Security includes

SOPHOS Cybersecurity evolved.

DNS BLOCK
INTERCEPT-X NGAV

GVA SECURE OFFICE

POWERED BY RAZOR TECHNOLOGY

GVA has teamed up with Razor to provide the most complete and secure technology package you need. Let us take care of the technology and you can focus on growing your business.

Reach out to the GVA team to get started!

operations@greatvalleyadvisors.com

Simple Support Plans and Focus

SIMPLIFIED BILLING

Services are billed on a per user basis monthly. We scale as you grow.

WE'RE YOUR TECH TEAM

Our support teams become your internal IT team. We're here for you 24 / 7 / 365.

TECHNOLOGY CHANGES

As tech changes, we work with you to make sure you're evolving with it.

BUSINESS FOCUSED

We will continue to provide ROI to your technology investment.

No industry is **safe** from the **threat** of cyberattacks.

43%

Conduct security awareness training.

52%

Have just a standard or sub-par recovery plan.

54%

Are somewhat satisfied with their security solutions.

42%

Blame their security issues on lack of training.

37%

Of attacks are related to phishing email issues.

60%

Are concerned they might be hit by a successful ransomware attack.

MJ /imagine technician fighting virus, cyber attack, threats, safety


ANATOMY OF AN ATTACK

Why Cyber Resilience Matters Today

What exactly is Cyber Resilience?

Cybersecurity resilience refers to an organization's ability to prevent, detect, respond to, and recover from cyber attacks, as well as the ability to continue operating during and after an attack.

Why is it so important?

Cybersecurity threats are becoming more sophisticated, frequent, and impactful, with the potential to disrupt business operations, damage reputation, and compromise sensitive information. Therefore, organizations need to be proactive and adaptive in their approach to cybersecurity, rather than relying solely on traditional security measures.

The Bigger Picture…

Traditional cybersecurity approaches typically focus on prevention and detection, but cybersecurity resilience goes beyond those measures to include response and recovery. It also emphasizes the need for continuous monitoring, testing, and improvement.

Traditional security is **no longer** working.

The Impending Storm of Cloud First, Security Third…

Cybersecurity can no longer be an afterthought

It must be the top of mind, always.

- Alert Fatigue →
- Configuration Issues →
- Lack of Visibility →

- Are companies investing in the right priorities?
- For a long time, cybersecurity was viewed as a technical problem, rather than seen as an operational risk and business continuity concern.
- Priorities are changing as breach implication become more significant, including emerging case law that now hold executives and business leaders accountable.
- Cloud adoption has moved from SaaS to Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), new security concerns are emerging when environments are improperly configured.

Cybersecurity is **not** a *one-size-fits all*… it’s multi-faceted.

MJ /imagine cyber security, cloud security, multi-faceted approach, 4k

Zero Trust Pillars

Governance

Identities | Endpoints | Apps | Infrastructure | Network | Data

Threat Protection

Understanding the Cyber Risks We're Facing

As the landscape evolves, so do the threats we face

Zero-day exploits:
Zero-day exploits are vulnerabilities in software or hardware that are unknown to the manufacturer or developers. Hackers can use these vulnerabilities to gain unauthorized access to systems or data.

Social engineering attacks:
Social engineering attacks use psychological manipulation to trick individuals into revealing sensitive information or taking other actions that can compromise security.

Advanced persistent threats (APTs):
APTs are long-term targeted attacks that are designed to steal sensitive information over an extended period of time. They can be difficult to detect and mitigate.

Malware:
Malware is a type of malicious software that is designed to harm or disrupt computer systems. It can take many forms, including viruses, worms, Trojans, and ransomware.

Phishing:
Phishing is a type of social engineering attack that uses email or other communication methods to trick individuals into revealing sensitive information such as passwords or credit card numbers.

DDoS attacks:
Distributed denial-of-service (DDoS) attacks are designed to overwhelm a website or network with traffic, making it unavailable to legitimate users.

Insider threats:
Insider threats occur when individuals within an organization misuse their access to sensitive information or systems. This can include intentional or unintentional actions that result in data breaches or other security incidents.

Cyber alignment is more critical then ever

The overall goal is to align people, process and technology to build resilient cyber defense architecture in line with business objectives.

Enforcing controls at all possible levels.


RAZOR
TECHNOLOGY
Delivering Digital Confidence
SECURITY
Protect Your World
Enhance cybersecurity **controls**.
Strategies for Strengthening Your Defense
MJ /imagine cyber security attack, end of services, service offline, hackers, 4k

Essential Security Controls

Keep your software and systems up to date

Keep your operating system, web browser, and software applications up to date with the latest security patches and updates. Cybercriminals often exploit vulnerabilities in outdated software to gain access to systems.

Use strong passwords

Use strong, unique passwords for each account or device, and use a password manager to securely store and manage your passwords. Strong passwords should be long, complex, and include a mix of letters, numbers, and symbols.

Enable multi-factor authentication

Multi-factor authentication (MFA) adds an extra layer of security to your accounts by requiring an additional form of authentication beyond just a password, such as a fingerprint, facial recognition, or a unique code sent to your phone.

Be cautious with email

Be cautious when opening email attachments or clicking on links in emails, especially if they are from unknown senders. Phishing emails often look like legitimate emails from trusted sources but contain malicious links or attachments that can install malware on your computer.

Backup and Test Recovery

Back up important files and data regularly to a secure location, such as an external hard drive or cloud storage service. This will help you recover your data in case of a ransomware attack or other data loss event.

Continue to Educate Employees

Educate yourself and your employees on cybersecurity best practices, including how to spot phishing emails and how to avoid falling victim to social engineering scams. Make sure everyone knows the importance of strong passwords, MFA, and other security measures.

It's important to understand where your weaknesses lie. When responding to an attack or breach, understanding how your organization may be exploited is a critical factor in prioritization.

The **evolution** of compliance – are you covered?

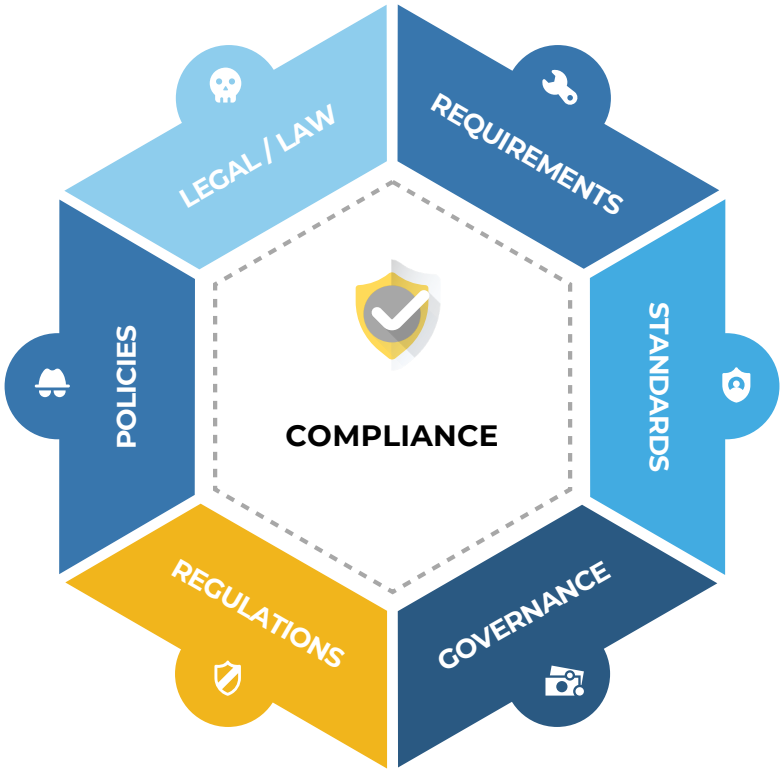
MJ /imagine document, compliance, security, cyber policy


RAZOR TECHNOLOGY
Delivering Digital Confidence
SECURITY
Protect Your World
The road to **hell** is paved in compliance obligations...
Being **prepared** is the key to avoid it.
MJ /imagine lonely road to hell, compliance, security, cyber policy

Till Death Do Us Compliance

- Previously security leaders were welcoming new advancements in compliance.
- Now we're met with confusion having to manage multiple cybersecurity and data protection laws and regulations.
- Customers are unsure which are the ones they should be implementing or are critical to their specific industry.

Can we learn to navigate the torrents of privacy and security regulations before we drown?



Effective Governance in Achieving Cybersecurity Compliance

Effective governance provides a structured approach for ensuring that cybersecurity compliance requirements are understood, implemented, and monitored. It also helps to ensure that cybersecurity risks are identified, assessed, and managed appropriately.

Current State

- Identify priorities
- Determine compliance requirements
- Review existing policies and practices
- Identify vulnerabilities and risk events

Assessment

- Identify threats
- Review vulnerabilities
- Define probability and like hood
- Categorize identified risks
- Create risk heat map

Target State

- Identify mitigation approaches
- Translate mitigation into desired outcomes
- Define goals for desired outcomes
- Review and outline security priorities

Roadmap

- Quantify and score current state
- Establish budget and identify resources
- Define targets within budget
- Share results with stakeholders

Continuous Improvement

Adopt next-gen cybersecurity tech

Holistic – Consider the full spectrum of information security, including people, processes, and technology.

Risk Aware – Understand that security decisions should be made based on the security risks facing their organization, not just on “best practice.”

Business Aligned – Demonstrate an understanding of the goals and strategies of the organization and how the security program can support the business.

Developing a practical roadmap that shows business value

- Identify the stakeholders who will be affected by the next-gen cybersecurity technologies implementation and define responsibilities based on skillsets and the degree of support.
- Adopt well-established data governance practices for cross-functional teams.
- Conduct a maturity assessment of key processes and highlight interdependencies.
- Develop a baseline and periodically review risks, policies and procedures, and business plan.
- Develop a roadmap and deploy next-gen cybersecurity architecture and controls step by step, working with trusted technology partners.
- Monitor metrics on effectiveness and efficiency

MJ /imagine cybersecurity , minimalist ,2D, sketch, background white

Techniques for Testing and Evaluating Plans

Testing and evaluating cybersecurity resilience is essential for identifying vulnerabilities, testing incident response plans, and ensuring that cybersecurity controls are effective in mitigating cyber threats.

Penetration Testing
Penetration testing involves simulating real-world cyber attacks to identify vulnerabilities and weaknesses in an organization's security controls.

Vulnerability Scanning
Vulnerability scanning involves using automated tools to scan an organization's systems and networks for known vulnerabilities.

Disaster Recovery Testing
Testing the infrastructure and systems that support the DR plan to ensure they are functioning as expected. This should include testing backups, failover systems, and recovery procedures.

Red Teaming
Red teaming involves using an external team of experts to simulate real-world attacks and test an organization's incident response capabilities.

Additional Important Policies:

- Information Security
- Business Continuity
- Access Control
- Incident Response
- Vendor Management
- Employee Training

Frictionless IT for business.

We've modified our DNA, from our platforms and services. Building concepts around open architectures, tools, cognitive communications and intelligence; we strive to empower our customers ecosystems and help establish business growth.


RAZOR
TECHNOLOGY
866.797.3282 | Razor-tech.com