

WELCH TIMES



SUMMER 2024

CONTENTS

4.
Welcoming new Team Members

8.
Blog:
Cyber Threats in Construction

10.
Blog:
Demystifying Cloud Security: Busting
Common Myths

12.
WCP Blog:
What is the role of an Investment Banker?

15.
Our Clients in the News

Welch LLP®

ACCOUNTING + TAX UPDATE

PRIVATE ENTERPRISES

October 9, 2024 | 10AM - 12PM

TAX
US TAX
HST/GST
ACCOUNTING
INTERNATIONAL FINANCIAL
REPORTING STANDARDS
ENVIRONMENTAL, SOCIAL, AND
GOVERNANCE

REGISTER

Gain insight for the year ahead.

OUR PEOPLE



DIANA WALSH, CPA, CA
PRINCIPAL, U.S. TAX ADVISORY SERVICES

Diana started her career in Halifax in 2005 after graduation from Dalhousie University. She has worked throughout the last 20 years in various services lines, having spent the majority of her career for the last 13 years assisting clients with US/Canada Cross Border personal tax. The areas include: compliance, planning, in-bound and out-bound planning, repatriation of US retirement account planning and personal advisory.

How has your experience with the Welch Team been going so far?
My experience with Welch LLP has been excellent - everyone is very welcoming and the focus on client satisfaction and overall team involvement with clients has been great to engage in.

What do you like most about your current role at Welch?
The direct client engagement and meeting with Welch colleagues and their clients and being able to add additional value to the conversations.

What do you look forward to the most in the next year?
Growing our US team and running some lunch and learns to give everyone more insight on the wonderful world of US Personal tax!

OUR PEOPLE



BOB MORRILL, CPA (MASSACHUSETTS)
SENIOR MANAGER, U.S. TAX ADVISORY SERVICES

Bob is a U.S. corporate tax specialist with over 30 years of public accounting experience. He has extensive experience in providing U.S. tax advice to public and private companies engaged in cross border activities. In addition to assisting companies with their U.S. tax compliance needs, Bob has advised companies on U.S. expansions, cross-border financing and cross border mergers and acquisitions. Bob has also assisted companies in evaluating their U.S. state tax obligations, including state income tax and sales tax filings. Bob has served companies in a wide range of industries, including many high tech and software/SaaS entities.

OUR PEOPLE



VIVEK GUPTA, MBA, CISA, CDPSE, CEH
*PARTNER & PRACTICE LEADER - TECHNOLOGY ADVISORY
WELCH ADVISORY PARTNERSHIP*

Vivek Gupta is the Practice leader for IT Advisory with a focus on IT Risk & Cybersecurity at Welch LLP. He specializes in delivering Technology Risk, IT compliance & Cybersecurity related services. Vivek possesses over 18 years of experience in cybersecurity, IT risk and compliance consulting functions delivering risk and controls related services to various clients in direct support of business objectives applying frameworks such as NIST, ISO 27001, PCI and CSA.

How has your experience with the Welch Team been going so far?
My experience at Welch so far has been extremely exciting and rewarding. I realized early on that Welch fosters a culture of collaboration, support and respect. I felt like I was welcomed into the family with open arms. The team here has been extremely supportive and open to ideas as I build the Tech Advisory business. I feel like I can reach out to anyone at the firm to get guidance as needed. I am grateful for the support I have received from my fellow partners. I can see that everyone here is vested in each other’s success.

What do you like most about your current role at Welch?
It is very entrepreneurial but at the same time, I also have the support as you get at a large firm. The ideology of Welch aligns with my personal beliefs, where I want my work to make a difference for our clients. We strive towards giving our clients the best value and ROI possible. As a Partner and Leader of the Technology Advisory practice, I like the fact that I am getting to build this business from a foundational level. I am enjoying the flexibility, the agility and the ability to pivot as the market evolves.

What do you look forward to the most in the next year?
I am looking forward to continuing to grow the business, add new service offerings, build a team and add value to our clients.

How can you
tell if your
security measures
are enough?

Get a Cybersecurity
Risk Assessment





Cyber Threats in Construction

The Rise of Ransomware & Digital Vulnerabilities

The construction industry stands at the intersection of innovation and vulnerability, going through ongoing transformation in both business processes and technological advancement. In recent years the construction industry has become more digitally focused. Construction firms are using digital tools not only to send invoices and plan projects from the back office, but also on site to build walls and foundations or to survey progress in real time. What was once created and collected manually, is now going digital.

Although technical advancements provide a lot of opportunities for growth, if left unregulated and unmonitored, it can also be a source of high risk. Unfortunately, the industry's lack of rigorous regulatory requirements and enforcement of data protection laws makes it an attractive target for cybercriminals looking to take advantage of the sector's strong reliance on digital tools to extort money. The infrastructure, bank accounts, personnel data, project data, and sensitive company information are at risk because of the lack of proper cybersecurity resiliency in place.

WHY IS THE CONSTRUCTION SECTOR SO HEAVILY AFFECTED?

- Lack of investment in cybersecurity infrastructure
- Complex Supply Chains
- Rapid Technology Integration
- Slow Regulatory Adoption
- Reliance on legacy systems
- Third-Party risks
- Lack of cybersecurity related regulations

There are robust strategies needed that can protect construction firms from cyber threats and safeguard systems, processes, data, customers, and brand. Implementing comprehensive security measures that not just cover endpoint security, but also advanced threat intelligence and network monitoring is crucial. These are some of the common strategies to protect an organization:

Employee Training & Awareness: Conduct regular cybersecurity training and awareness sessions for construction staff to educate them on potential risks and best practices. Encourage employees to be vigilant and report any suspicious activities promptly.

Regular Software Updates: Keep all software, including operating systems, applications, and security tools used in construction projects and office operations, up to date to patch known vulnerabilities.

Firewalls & Antivirus Software: Implement robust firewall and antivirus solutions to detect and block threats. Ensure that these tools are regularly updated and configured properly.

Data Encryption: Encrypt sensitive data both in transit and at rest to protect it from unauthorized access, including project plans, client information, and financial data.

Access Controls: Enforce strong access controls with role-based permissions. Limit access to sensitive data and systems and implement MFA to access systems or data.

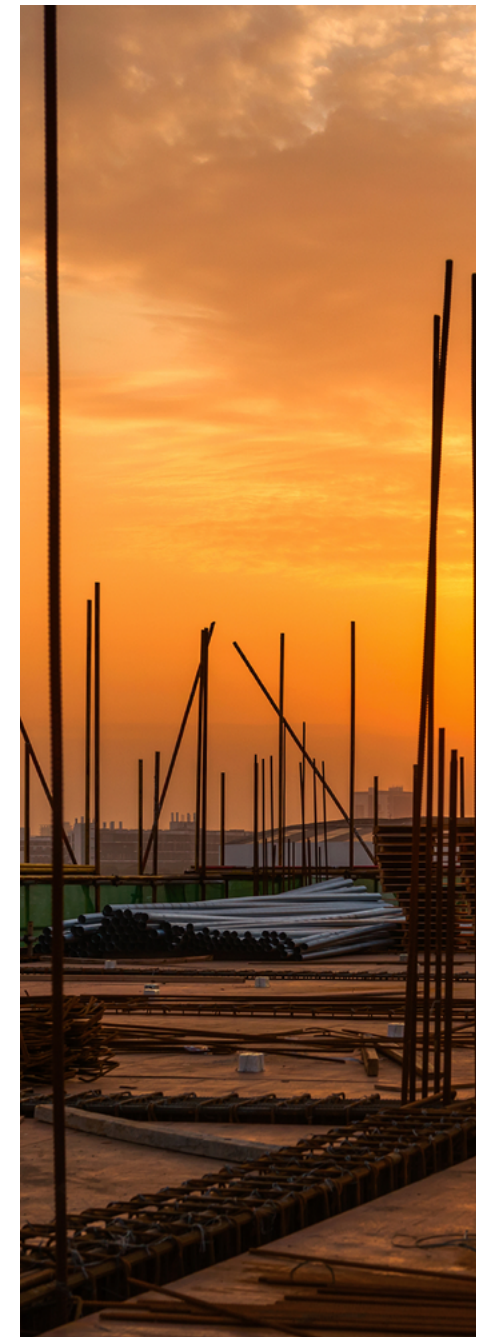
Backup & Recovery: Regularly back up critical data and test the backups to ensure they are functional. Create a disaster recovery plan to expedite data restoration in the event of an attack.

Incident Response Plan: Create a comprehensive incident response strategy outlining measures to follow during a cyberattack. Regularly test and update this plan and conduct tabletop exercises with scenarios relevant to the construction industry.

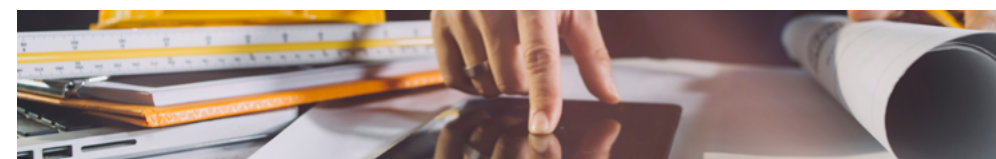
Vendor Security: Assess the cybersecurity practices of third-party vendors and partners, such as subcontractors and suppliers, to verify they satisfy security standards, as they typically have access to critical project information.

Regular Audits & Assessments: Conduct periodic security assessments and audits of construction management software, on-site devices, and office systems to identify vulnerabilities and weaknesses. Address these issues promptly to enhance security.

Cybersecurity Policies: Develop and enforce cybersecurity policies and procedures tailored to the construction industry's needs and risk profile, ensuring all employees and partners understand and adhere to these guidelines.



By embracing robust protective measures, the pillars of progress and security can stand together, ensuring a resilient future in the face of ever-evolving cyber-attacks.



Busting Common Myths

Cloud computing has become a critical aspect for nearly every modern-day operation, providing businesses with both an agile environment to scale, as well as the flexibility to deploy only what they need. However, as organizations increasingly rely on cloud services, misconceptions and myths about cloud security have proliferated. Let's debunk some of the most common myths surrounding cloud security to help you make informed decisions and safeguard your digital assets.

1 CLOUD PROVIDERS ARE SOLELY RESPONSIBLE FOR SECURITY.

Reality: While cloud service providers (CSPs) like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) do provide robust security measures, the responsibility for security is shared. The "Shared Responsibility Model" dictates that customers are responsible for securing their data and applications in the cloud. CSPs ensure the security of the cloud infrastructure itself.

2 THE CLOUD IS LESS SECURE THAN ON-PREMISES SOLUTIONS.

Reality: Cloud providers invest heavily in security, often exceeding the security capabilities of on-premises data centers. However, the security of a cloud environment depends on how well it is configured and managed by the customer. Misconfigurations, poor access controls, and inadequate security practices can compromise cloud security.

3 DATA IN THE CLOUD IS ALWAYS ENCRYPTED.

Reality: While many cloud providers offer encryption options, data is not always encrypted by default. Customers must configure encryption settings, manage encryption keys, and ensure data protection according to their specific requirements. This is particularly important for sensitive or regulated data.

4 CLOUD OUTAGES MEAN DATA LOSS.

Reality: Cloud providers have robust redundancy and backup systems in place to minimize data loss during outages. However, data loss can occur if customers do not implement proper backup and recovery strategies. It's essential to understand the provider's Service Level Agreements (SLAs) and have a contingency plan in place.

5 THE CLOUD IS NOT COMPLIANT WITH REGULATIONS.

Reality: Leading cloud providers offer services and features designed to help customers meet various compliance requirements, such as GDPR, HIPAA, and SOC 2. However, customers must configure and manage these services properly to ensure compliance. Compliance is a shared responsibility.

6 CLOUD ADOPTION AUTOMATICALLY INCREASES SECURITY RISKS.

Reality: Cloud adoption does introduce new security challenges, but it also offers enhanced security capabilities. Many cloud providers offer advanced security features like identity and access management, network security, and threat detection. When configured correctly, cloud environments can be highly secure.

7 CLOUD SECURITY IS EXPENSIVE.

Reality: Cloud security costs can be managed effectively based on your organization's needs and budget. Cloud providers offer scalable pricing models, allowing you to pay for only the security services you require. Effective security investments can reduce the risk of costly security breaches.

8 CLOUD SERVICES ARE ALWAYS VULNERABLE TO DDOS ATTACKS.

Reality: While cloud services can be targets of Distributed Denial of Service (DDoS) attacks, cloud providers typically have robust DDoS protection in place. Customers can also enhance protection by configuring security groups and using Content Delivery Networks (CDNs).

9 MOVING TO THE CLOUD AUTOMATICALLY SOLVES SECURITY PROBLEMS.

Reality: The cloud is not a silver bullet for security. Migrating to the cloud requires careful planning and security considerations. The same security principles that apply to on-premises environments, such as access control, data encryption, and monitoring, are essential in the cloud.

10 CLOUD SECURITY IS A ONE-TIME EFFORT.

Reality: Cloud security is an ongoing effort. Threats and regulations evolve, and cloud environments change. Regular security assessments, audits, and updates are essential to maintain a strong security posture in the cloud.

Whether an organization is just beginning its cloud adoption journey or undergoing the process to enhance their cloud footprint, it is crucial to dispel common myths about cloud security. Understanding the shared responsibility model, implementing best practices, and staying informed about cloud security advancements are key to ensuring a secure and successful cloud adoption. By addressing these misconceptions, organizations can confidently harness the benefits of cloud computing while maintaining robust security measures. Talk to our experts on how Welch's cybersecurity team can help ensure that your cloud environment is secure.



What is the Role of an Investment Banker?

As you embark on the journey of selling your business, you will want to make sure you have the right people on your team. This starts with the investment banker / M&A advisor. This blog outlines the role that the investment banker will play as you navigate the process of selling your business.

INITIAL ANALYSIS

An investment banker's role starts before entering the market to sell your business. Their first task is often explaining the process to business owners, giving them market insights, and setting expectations. They might even advise that now is not the right time to take your business to market, citing reasons such as prevailing market conditions, business performance, or the quality of information readily available.

PREPARING FOR MARKET

If the time is right for selling, an investment bank will start preparing materials that will be used to profile your business to prospective buyers. The primary document used for narrating your business's story is termed a confidential information memorandum (CIM). A well prepared CIM will allow a buyer to make an objective evaluation of your company.

Containing sensitive information, the CIM is withheld from buyers until the execution of a non-disclosure agreement (NDA). Consequently, the initial communication with buyers occurs through a teaser, which provides a condensed version of your story – akin to “Coles Notes.” The investment banker will prepare the teaser ensuring it gives a buyer enough information to generate interest without divulging who exactly you are.

MARKETING

Your investment banker plays a pivotal role in compiling a list of prospective buyers to share the teaser with. This list typically encompasses financial buyers (such as family offices and private equity firms) and strategic buyers.

The banker will then take the deal to market, overseeing initial communications and dialogues. They ensure the execution of NDAs with interested parties and distribute the CIM. As discussions progress, prospective buyers typically express a desire to meet with the owner and management, a process facilitated by your investment banker.

Ultimately, the objective of the investment banker is to orchestrate a competitive process aimed at enhancing the value of your business.

SELECTING A BUYER

If everything proceeds according to plan, you can expect to receive multiple offers to evaluate. Your banker will assist in this evaluation process, offering guidance and taking the lead in negotiating with the remaining prospective buyers. Eventually, a definitive step forward will be taken by entering into an exclusive letter of intent (LOI) with one party, followed by a final push to close the deal.

LOI TO CLOSE

Once an LOI is entered into, the buyer is going to want to perform due diligence to confirm that everything presented to date in the CIM, teaser and other communication is true. This phase can be extensive and demanding. While you control access to your information, your investment banker should have been assisting you in preparing for the due diligence process. A competent banker can expedite this process by anticipating the requests and providing guidance around how to best present the information.

While diligence is happening, the legal documents will be prepared, and any necessary tax planning will be getting finalized. At this point, your banker will take on the role as project manager, ensuring all the various service providers are working together to get the desired deal across the line. For further insights into the parties involved in a transaction, please refer to our blog post on assembling your deal team.

Many business owners go through an M&A transaction once in their life while others are more experienced. Nonetheless, a strong investment banker is critical to ensuring the deal runs efficiently, and that value is maximized.

Please contact cenman@welchcapitalpartners.com to learn more about our experience with successfully closing transactions.

Welch LLP®

ACCOUNTING + TAX UPDATE

NON-PROFIT ORGANIZATIONS

November 6, 2024 | 10AM - 12PM

REGISTER

Our expert speakers explore issues related to Accounting and Tax Standards, along with other topics vital to your non-profit organization to help you prepare for the upcoming year.

This year's event agenda will include:

TAX

RISK RESERVES

ACCOUNTING

HST/GST

ENVIRONMENTAL, SOCIAL, AND GOVERNANCE

our CLIENTS IN THE NEWS



FOOD CYCLE SCIENCE

RAISES MILLIONS IN FRESH FINANCING TO FAST-TRACK “TABLE-TO-FARM” TECH



RVezy

ON THE ROAD

Welch LLP®

Risk Advisory
Welch LLP

ELEVATE

BY WELCH LLP

Welch
Capital
Partners

 FAMILY WEALTH
ADVISORY BY WELCH LLP

welchllp.com