rma Risk Management Association
Long Island Chapter

Spring 2023 | Volume 1.18

“An investment in knowledge always pays the best interest.”
- Benjamin Franklin

A Message From Our President

Happy spring! I have some good news to share. Our signature Annual Panel Discussion is approaching (April 21st), marking the 1-year anniversary of our return to in-person events. I remember anxiously monitoring registrations last year and ultimately being rewarded with the unconditional support of the Long Island business community. That support has continued through each of our subsequent events and my heartfelt thanks to all of you who keep the RMA LI Chapter vibrant and thriving.

We have another great panel lined up, making me optimistic that we can exceed last year’s attendance of 100-plus audience members.

Our panelists:

- Melissa Acosta Hotzoglou, Managing Director and Head of Corporate Sales US CMB, HSBC Bank USA, National Association
- Jason Lipiec, Long Island Market President, M&T Bank
- Lou Mastrianni, Head of Commercial Banking-North Region, Capital One
- Rob D. Bryant, Region Manager, Metro NYC and Long Island, Chase Bank

Our Young Professionals continue to host great networking events. They hope to see you on May 4th for their Cinco De Mayo celebration at Cara-Cara Mexican Grill in Farmingdale.

Our Chapter Board gathers every May for its annual planning session. I encourage your feedback and thoughts prior to the session. What topics would you like to see presented? What format changes should we consider? Do you have young professionals in your organization that are looking to get involved?

Did you know that the RMA LI Chapter awards various scholarships each year for local college students who are pursuing degrees in business and finance? Help us get the word out. You can connect with us directly at: rmalongisland@gmail.com.

Wishing you a wonderful spring holiday, and we will see you April 21st.

Sincerely,

Michael Heller

OUR SPONSORS

bakertilly

BA Brown Altman & DiLeo, LLP

CB CertilmanBalin Attorneys

Crowe

MARCUM
ACCOUNTANTS ▲ ADVISORS

GRASSI
ADVISORS & ACCOUNTANTS

MH&H Moritt Hock & Hamroff LLP
ATTORNEYS AT LAW

MEI Middleton Environmental Inc.
Environmental Consultants and Engineers

M&T Bank
Understanding what’s important®

RivkinRadler LLP
ATTORNEYS AT LAW

Save the Date

2023 Annual Panel Discussion
Date: April 21, 2023, 8am – 10am
Venue: Radisson Hotel Hauppauge
Register here

RMA LI - Young Professionals

Cinco de Mayo
Date: May 4, 2023 6pm– 8pm
Venue: CaraCara Mexican Grill, Farmingdale NY
Register here

Annual Sponsorships Still Available

For information regarding Sponsorship please contact:
Neil Seiden at neil.seiden@assetenhancement.com
or call 516-767-0100

RMA Scholarships

James T. McCarthy Scholarship - $2,500
Dr. Pearl Kamer Scholarship - $2,500
Patrick M. Demery Bankers' Lifetime Achievement Award - $1,500

Application deadline: May 1, 2023

Eligibility:

Bankers and students interested in pursuing their education and career in the area of banking, comercial lending or credit risk management. You must be enrolled at an accredited college, pursuing a pertinent degree program.

Application package must include the following:

- College transcript and evidence of current enrollment at an accredited college
- Essay from applicant stating:
  - Why you have chosen or are interested in a career in banking
  - Your career goals and how this scholarship will help you meet your goals
- Employment history and current job description, if applicable
- Extracurricular activities, community service
- List of leadership positions, honors and awards
- Letter of recommendation from your current employer or professor

Note: Incomplete application packages will be disqualified.

Applications will be reviewed by the
Scholarship Committee of the
Long Island Chapter of Risk Management Association.

Forward questions or your completed application package to:
Bonnie Dougherty, Senior Vice President
Valley National Bank
BDougherty@valley.com

Join. Engage. Lead

ERP Best Practices for Manufacturing & Distribution Companies

Part I: Selecting and Implementing an ERP System

Hassan Khan,
Anthony D'Agostino
Danielle Marchese
Grassi

Developing a comprehensive systems strategy is critical to every company's long-term success. But the effectiveness of the strategy is only as good as the selection and implementation processes that precede it. This is especially true when choosing and rolling out an enterprise resource planning (ERP) system.

An ERP system is software that automates, integrates and streamlines business processes across an organization, making accounting, data analysis and other operations more efficient. The benefits of ERP have a direct impact on the customer experience, which makes it one of the most important technology decisions you will ever make for your manufacturing or distribution company.

Before you embark on an ERP project, ask yourself why you are implementing the system in the first place, and communicate your answer to all stakeholders – upper management, project team, ERP vendor and, eventually, all employees. This will provide a solid foundation for consensus-building, change management, adoption, long-term usage and maximum return on your investment.

It is also important to understand key ERP selection and implementation best practices from Day 1 – before you even start to evaluate or install a new system.

Get ERP Selection Right

The variety of ERP software available in today's marketplace makes the selection process challenging. Choosing an ERP system requires a thorough, structured and unbiased decision-making process that includes the following steps:

Define Clear Requirements. The best place to start is to define your goals and link them directly to the ERP features that will achieve them. If the goal is to save time and lower costs, automation features will most likely be a requirement. If your objective is to improve customer communication or analysis across the business, certain data management tools may be must-haves.

Assess Current Environment. Analyzing existing systems, workflows, and critical business processes is another best practice that can uncover deficiencies that the ERP system should address. Typically, a management team will assess all of the shortcomings of a company's performance and prioritize those items based on visibility to the customer and impact on the customer's experience.

Narrow down your options. Shortlist and evaluate at least four different ERP systems to find the best match to the identified requirements and needs. Looking at systems that are customized to the M&D industry, or your sub-sector, is a helpful way to hone in on your best options.

Evaluate the impact on your workforce. When making your decision, don't forget to consider the impact on your workforce. ERP upgrades often require a client to hire more staff to maintain a more robust system than what was used previously. You should also consider the abilities of the existing team to work with the new ERP. Conversely, depending on the level of automation and process improvement provided by the system you select, the change may lead to necessary layoffs or increased training expenses. All of these factors should be considered as part of your overall decision-making process.

Continued...

Communicate with your workforce. Before the selection of a software infrastructure is even made, you want to communicate the reasoning for this change, manage expectations about the project and proactively address any negativity and concern.

The Do's & Don'ts of ERP Implementation

ERP implementation can be equally complicated and often requires extensive planning, training, and support to achieve the intended results. The implementation team needs to understand all of the needs and workflows defined in the selection process to realize the full potential of the ERP solution. Follow these best practices to achieve maximum results:

Don't treat your ERP implementation as an IT project. The most effective implementation will be a "people" project. ERP projects are done by you, not to you.

Do define clear project scope and goals. While the objectives of the ERP will be clearly laid out in the selection phase, this is the time to take it a level deeper. Which specific modules are you implementing? Which areas of your business will be affected? Which systems will require integrations to your new ERP? Are you doing this all at once or in sequence? Without answering these questions up-front, your budget can spin out of control and your ERP suppliers will not have a clear understanding of clear goals and key performance indicators (KPIs).

Do obtain executive buy-in. Successful ERP implementation requires cross-functional collaboration and the reallocation of budget and resources throughout the implementation process. Getting executive buy-in ensures senior stakeholders understand the long-term benefits and how this will impact top-level business goals such as revenue and profitability. Successful buy-in ensures executives are fully committed to seeing the project through – from planning to long-term support, and every decision in between. A member of senior management should be assigned as a "project sponsor" to help make decisions on priorities and trade-offs of resources and help facilitate ongoing executive support.

Do assign a core project team. Your ERP project team is the most critical factor in your implementation. They will establish goals, requirements, and key performance indicators (KPIs), as well as carry out daily project management tasks. These people need ample time, support, and skills to perform the implementation effectively and avoid delays, growing costs and configuration missteps. In addition to the project sponsor, the core project team should consist of a project lead supported by a core team of functional/departmental leads or members who are knowledgeable about the company's processes and/or have completed an ERP project before.

Don't customize – configure. A key ERP implementation best practice is to conform to the standard business processes of your new ERP system as closely as possible. Doing so will make the implementation quicker, the maintenance costs cheaper, and future upgrades easier. In rare instances, customizing a business process makes sense, but if you find yourself customizing processes frequently, there is a good chance you chose the wrong ERP system in the first place.

Do clean data before migration. It is important to make sure the formatting of the data in a new ERP system is correct before importing data from your existing system. The process of cleaning legacy data before migration includes ensuring existing tables and databases are correctly formatted before they are imported and removing redundant data that provides little value.

Data can be transferred to the new ERP system manually or via automation. Automation is faster and less tedious but still needs plenty of oversight to avoid issues. Your ERP partner, IT staff and implementation team will all need to be involved for a successful data migration.

Do test system before deployment. Testing your ERP system before deployment is important in ensuring that it is fit for purpose and able to replace your legacy systems. This will include unit testing for each part of the system, integration testing to determine if these parts work together, and system testing to ensure that the entire system operates as expected. Alongside technical testing, it is also important to develop a full UAT (user acceptance testing) plan that allows actual end-users to test the ERP system before it is fully implemented.

A successful ERP implementation can bring invaluable improvements to customer satisfaction, productivity, cost containment and more – but not without a lot of planning and sacrificing first. Your budget, people and processes will all be impacted initially, but by continually communicating the benefits, securing buy-in from the top, defining goals and managing change, you can avoid the obstacles that hamper the efforts of even the most qualified project team.

10 risks and cybersecurity strategies for banks in 2023

David R. McKnight
Timothy Tipton
Crowe LLP

Cryptojacking, AI-based attacks, ransomware, and phishing are among the threats for 2023. Specific cybersecurity strategies can help banks prepare.

Cyberattacks are becoming more frequent, and they're costing companies more as well. The average cost of a data breach for a U.S. company in 2022 was $**9.44 million, up from $9.05 million** the previous year. As the financial services sector grows more digitized and the volume of electronic transactions surges, the industry is even more susceptible to cyber-based perils.

In 2023, 10 cybersecurity hazards in particular could cause significant disruption, but financial services companies can implement specific, proactive cybersecurity strategies to mitigate risk.

Ransomware Attacks

Ransomware attacks are becoming more frequent and sophisticated, and financial services organizations are prime targets for cybercriminals. These attacks can cause serious harm to organizations, including sensitive data loss and operational disruption. Additionally, some organ izations are forced to pay millions of dollars in ransom payments to threat actors.

Key prevention and mitigation strategies:

- Apply multilayer security measures such as firewalls, intrusion detection, and prevention systems
- Continually monitor and assess security practices
- Update and patch software and systems on a regular basis Encrypt data and devices
- Provide employee security training and awareness programs Create a detailed incident response plan
- Implement strong backup and disaster recovery procedures

Continued...

Cloud Security Threats

Cybercriminals are taking advantage of financial services companies' increasing embrace of and reliance on cloud services, so cloud security controls are critical. Oncethreat actors gain entry to these cloud services, they target sensitive information, which they then alter, steal, destroy, or use to gain reverse access to the organizations' internal networks.

The most serious vulnerabilities often stem from cloud misconfigurations, unrestricted cloud management platform access, and lack of visibility of cloud infrastructure. The resulting attacks can expose sensitive information, grind operations to a halt, and inflict substantial financial losses.

Key prevention and mitigation strategies:

- Engage a cloud access security broker (CASB) that can provide an extra layer of protection between the cloud service and the organization's network
- Work with the CASB to monitor and enforce security policies and provide visibility into and control over cloud use

Artificial Intelligence and Machine Learning Attacks

As fast as financial services companies are figuring out ways to apply artificial intelligence (AI) and machine learning to benefit their businesses, cybercriminals are also devising ways to weaponize these tools for more efficient cyberattacks. The automated and persistent nature of these attacks can make them especially hard to detect and defend against.

Some of the most frequent types of AI and machine learning attacks that financial services companies face include:

- **Adversarial attacks and data poisoning.** In these types of attacks, threat actors manipulate input data or training data, causing machine learning models to produce incorrect results or behave in unintended ways.
- **Model theft.** Cybercriminals steal a machine learning model and use it for malicious purposes.
- **Model inversion.** Threat actors reverse-engineer a machine learning model to extract sensitive information.
- **Bias and fairness attacks.** Cybercriminals manipulate data or models to create systematic biases or unfairness in the results from machine learning algorithms.

Bias and fairness attacks. Cybercriminals manipulate data or models to create systematic biases or unfairness in the results from machine learning algorithms.

Key prevention and mitigation strategies:

- Protect models through adversarial training specifically designed to test resilience to attacks
- Regularly update and retrain models on adversarial responses Encrypt data, both in storage and during transmission
- Apply secure protocols such as HTTPS and TLS to prevent unauthorized data access to data

Continued...

InsiderThreats

Employees, vendors, and other individuals who have access to sensitive information can pose a risk to an organization – whether they intend to or not.

Insider threats can take various forms. Sometimes, individuals misuse sensitive information for personal gain, such as theft of confidential customer data or intellectual property for financial profit. But other threats come from more innocent and accidental actions, such as someone sending an email containing confidential information to the wrong recipient.

In just two years between 2020 and 2022, the number of insider threat incidents worldwide rose by 44%.

Key prevention and mitigation strategies:

- Conduct thorough background checks on all employees and due diligence in vendor management
- Provide regular security awareness training
- Implement strict access controls to sensitive information
- Lean on technology solutions such as data loss prevention tools and activity monitoring software

Phishing Attacks

Phishing attacks trick individuals into disclosing sensitive information such as login credentials, financial information, and personal details. Increasingly sophisticated techniques and messaging have made these phishing attacks more effective and persuasive than ever.

The cost of a phishing attack can vary widely depending on factors such as the size and complexity of the bank or other financial services company, but the total financial impact to the organization can easily add up to a multimillion-dollar figure.

Key prevention and mitigation strategies:

- Implement robust security solutions such as email filtering, multifactor authentication, and URL filtering
- Train employees to recognize and report phishing emails
- Provide additional training on topics such as safe browsing practices and optional security features
- Build a well-defined incident response plan
- Work closely with law enforcement to investigate any attacks

Continued...

Legacy System Attacks

Legacy systems are systems that have reached an end-of-life or end-of-support stage from the vendor, making them vulnerable to security threats. These older systems often lack defenses against the latest and most sophisticated threats to cybersecurity in banking, so organizations that use legacy systems risk security breaches and data loss.

Spending on legacy systems can drain IT resources, too. Between 2010 and 2020, about three quarters of IT spending by corporations and governments worldwide went toward operating and maintaining existing IT systems.

Key prevention and mitigation strategies:

Banking leaders and their cybersecurity teams must work together to address the problems of legacy systems.

- Assess the organization's technology landscape
- Devote the necessary resources to modernize systems

Cryptojacking

Cryptojacking occurs when a cybercriminal gains unauthorized access to an organization's computing resources and uses them to mine crypto assets.

These attacks are becoming increasingly prevalent, and the impact of cryptojacking on an organization's systems can add up fast. Cryptojacking can cause substantial performance degradation, eat up resources, and lead to slowdowns. In addition, the criminal's theft of computing power and electricity can result in higher utility and technology costs.

Key prevention and mitigation strategies:

Organizations need to take proactive measures against cryptojacking threats.

- Implement robust security measures
- Regularly monitor systems for signs of suspicious activity

Continued...

Internet of things (IoT) Security Limitations

In the past few years, more financial services companies have woven IoT devices into their infrastructure and operations. As a result, IoT is rapidly transforming how financial services organizations function, from point-of-sale systems to smart locks, wearables, building automation systems, and mobile devices.

However, this rapid proliferation has also created new cybersecurity risks that organizations must address. Despite the widespread adoption of IoT devices in the financial services industry, these devices often come with few security measures. Many devices lack basic security features such as encryption, authentication, and access controls. These security limitations make some IoT devices a soft target for cybercriminals.

Key prevention and mitigation strategies:

- Assess where IoT is being used within the business
- Limit access of IoT devices to the information and systems needed to perform their functions
- Build a comprehensive plan to manage and secure all IoT devices

Supply chain attacks

Cybercriminals often explore supply chains and exploit the weakest security link by compromising software, hardware, or other system components before information gets delivered to the end user. The results of these attacks can be devastating, with consequences ranging from data breaches and theft of sensitive information to disruption of operations.

In 2022, the average cost of a supply chain attack was $4.4 million, and the average life cycle of an incident for U.S. companies lasted 303 days – 26 days longer than the global average.

Key prevention and mitigation strategies:

- Perform due diligence and risk assessments for all suppliers
- Apply secure software development practices
- Create a strategy for regular monitoring and detection of potential supply chain risks
- Consider using only secure hardware, software, and services from trusted suppliers
- Implement secure configurations and access controls
- Build an incident response plan that identifies critical assets, establishes clear roles and responsibilities, and outlines contingency plans

Continued...

Blockchain Security Gaps

Blockchain technology has revolutionized the financial services industry, but it has also created new security risks.

Blockchain networks contain multiple elements that companies must manage and secure, including the underlying infrastructure, the cryptographic algorithms and protocols used to secure transactions, and the consensus algorithm used to validate transactions and maintain the integrity of the blockchain. Smart contract security represents another critical concern, as blockchain networks use these contracts to automate transactions and enforce rules.

Key prevention and mitigation strategies:

To bolster the security of blockchain-based systems in the financial services industry, banks must regularly evaluate the overall security of these systems and their components.

- Conduct security assessments and testing to identify potential vulnerabilities
- Implement remediation measures for any identified issues

How Construction Companies Can Prevent Cyberattacks

Michael Needham, Supervisor, Marcum LLP

With each wave of new technology, companies become more automated and efficient — and more vulnerable to cyberattacks. Construction companies are no exception, and in fact, companies in this sector make for particularly appealing targets for a handful of reasons:

- **Construction companies store large amounts of sensitive data,** especially those that work on government contracts. This data could include bidding strategies or highly sensitive blueprints.
- **Many construction companies use software and/or devices that could contain vulnerabilities.**
- This includes job costing systems, time and entry systems, and asset tracking software.
- **Construction companies frequently work with numerous vendors and subcontractors.** A data breach could affect any of these partnered companies.

For example, in 2019 Bird Construction was allegedly targeted by cybercriminals. The hackers stole 60 gigabytes of data, including social security numbers, banking details, names, email addresses, and health information. An attack like this could easily disrupt business operations, costing a company time and money — not to mention its trust and reputation within the industry.

An IBM study found that 74% of construction-elated companies are not prepared for a cyberattack.[1] In reality, even those that are prepared must stay vigilant because a motivated cybercriminal may eventually find their way in.

Here are a few steps companies can take to prevent cyberattacks:

- **Educate your employees.** Companies should train staff to recognize potential cyber threats. Instructions for what to do in the event of a potential attack should be well-documented.
- **Make sure employees use complex passwords and change them regularly.** This helps deter cybercriminals from accessing company systems.
- **Install proper malware and anti-virus software and keep it updated.** This helps protect sensitive data, including social security numbers, bid information, and customers' and vendors' personal information. Make sure all systems are up to date and tested for possible breaches.
- **Hire an outside IT firm to test the system and recommend improvements.** This tends to be costly but very effective.

In the digital age, companies in almost every industry are susceptible to cyber threats. Mitigating that risk sometimes requires investing significant resources, but it can save millions of dollars in the long run.

[1] Gavejian, J. C., & Lazzarotti, J. J. (2022, April 1). Construction industry: Data security considerations. The National Law Review. Retrieved October 31, 2022, from https://www.natlawreview.com/article/construction-industry-data-security- considerations

2022-23 RMA-LI OFFICERS

PRESIDENT
Michael Heller
Rivkin Radler, LLP

TREASURER
Paul Becht
Baker Tilly US, LLP

SECRETARY
Sylvia Kachala
Bank of America, N.A.

VICE PRESIDENT
Richard Romano
Valley Bank

ASSISTANT TREASURER
Paul DiTredici
Marcum LLP

ASSISTANT SECRETARY
Victoria Scolaro
Bank of America, N.A.

2022-23 RMA-LI DIRECTORS

Jennifer Acerra
Citibank, N.A.

Toni Badolato
M&T Bank

Joan Brigante
Retired

Alison Burke
Valley Bank

Bill Conlan
HSBC Bank USA, N.A.

Peggy Coppola

Matt Crennan
Dime Community Bank

Bonnie Dougherty
Valley Bank

James Goldrick
Pursuit

Rob Grote
Grassi

Marc Hamroff
Moritt Hock & Hamroff LLP

Jeannette Hug
M&T Bank

Michael Kid
M&T Bank

Keith Lawlor
TD Bank

Barbara Liguori
Capital One Bank

Theresa McCarthy
Dime Community Bank

Robert Milas
Wells Fargo Bank

Roger Rose
Dime Community Bank

David Saunders
Asset Enhancement
Solutions, LLC

Neil Seiden
Asset Enhancement
Solutions, LLC

Brian Stone
M&T Bank

RMA YOUNG PROFESSIONALS COMMITTEE OFFICERS

Roger Rose
Dime Community Bank

Keith Annunziata
Gettry Marcus CPA,P.C

Brian Boland
Moritt Hock &
Hamroff LLP

■ Newsletter Editor: Bill Conlan, HSBC Bank USA, N.A.