Key Cyber Risks at the ERP Level

Process & Industrial Products (P&IP) Sector

December, 2014
Today’s presenters

Bhavin Barot, Sr. Manager
Deloitte & Touche LLP

Goran Ristovski, Manager
Deloitte & Touche LLP
Agenda and Objectives

Areas of Cyber Risk within ERP and P&IP Sector

Emerging Cyber Risk Triggers, Issues and Opportunities

Enterprise Resource Planning (ERP) within organizations and key trends
  • Application Security Monitoring
  • Expanding Application Ecosystems
  • Managed Services
  • Preventing Cyber Attacks

Next Steps
  • What can you do to help your organization?
Areas of Cyber Risks

There is a preponderance of ERP platforms in the P&IP Sector. Cyber is at the heart of these environments.

Changing the game on cyber risk

• Most reports on cyber risk revolve around a common theme: despite heightened attention and unprecedented levels of security investment, the number of cyber incidents — and their associated costs — continues to rise. They typically point to the growing sophistication of hackers and other adversaries as a particularly intractable problem, and some consider whether being secure is even possible in today’s rapidly evolving landscape of cyber-attacks. Compound this fact with the constantly changing technology landscape, and you have a challenge that can become exceptionally complex for many ERP centric companies.

Enterprise Application Integrity is at the core

• Companies are focused on competencies to address the ever-changing technology ecosystem, including the move of applications to the edge, the increasing application layer cyber threat, and the growing analytics opportunity for continuous security and control monitoring. They do this through core application security and controls design work, with focus on application and control monitoring, Governance, Risk and Compliance (GRC) data analytics, and enterprise application resiliency.
P&IP industry is evolving – Is your company protected?

The need for a more integrated supply chain is driving producers to “open up” ends of their supply chain to outside vendors and customers – these connections and relationships must be adequately secured to protect the organization.

Recent cyber attacks highlight the urgency for organizations to contend with ever increasing risks to customer protection, continuity, fiduciary responsibility and operations. Cyber issues lead to brand degradation and change in consumer behavior.

Increased government and environmental regulations can have an effect on organizations dealing within the P&IP sector – greater emphasis must be placed on validating that organizations are compliant with all applicable regulations.

The consolidation of companies within the sector can lead to system integration challenges when dealing with divided systems. The combination of two organizations intellectual property needs to be tightly controlled.
## Cyber Risk Triggers, Key Issues and Opportunities

The following market triggers and trends within P&IP are classic enablers for addressing Cyber Risk issues:

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Key Issues &amp; Opportunities</th>
</tr>
</thead>
</table>
| **System Integration**                       | • The need for combining outdated siloed systems increases the need for consolidated business processes  
• *Technology components must be secured and structured so that business process data and operations can operate smoothly*                                                                                                                                                                                   |
| **Data classification and Protection**       | • P&IP data regarding margins, costs and manufacturing processes are typically regarded as highly sensitive  
• *The access and handling of this data needs to be controlled to authorized personnel*                                                                                                                                                                                                              |
| **Trade Secret Protection**                  | • Competition in the P&IP sector and the protection of key formulas and recipes is often regarded as the most critical asset a company possesses  
• *The access and handling of this critical data needs to be restricted to limited authorized personnel and monitored*                                                                                                                                                                          |
| **Government and environmental Regulations** | • Heavy regulations or responsibility for the storage of other organization’s data cause more legal requirements and potential penalties  
• *Systems need to be setup to comply with all regulations*                                                                                                                                                                                                                                           |
| **Mergers and Acquisitions**                 | • Integration of technology systems and/or processes with a child company’s users, systems and/or processes is a struggle  
• *Systems need to be built so they are scalable for future growth*                                                                                                                                                                                                                            |
| **Business Continuity**                      | • Incident (internal or external) brings the system to a standstill  
• *Prevent impact on business operations and have resiliency programs ready for deployment after an incident*                                                                                                                                                                                                       |
ERP within the P&IP Industry
Expanding Value

The traditional monolithic, Information Technology (IT)-driven world of ERP that most organizations inhabit today is coming under siege sooner than expected as the business continues to question the value they receive from their ERP investments, users complaints of inflexible and unfriendly processes, and ERP vendors struggle to deliver innovation.
Key ERP Trend 1 – Application Security Monitoring

Overview

Companies desire to be more proactive in preventing events within the IT landscape, including threats in their ERP environment. They are moving toward real-time, up-front, preventative, monitoring of enterprise application user activity to identify trends and vulnerabilities within their core business applications. Reacting to incidents after they occur, in a detective fashion, is no longer an option in the fast-paced and ever changing world of cyber risk.

Impacts

Real-time monitoring of ERP security, controls and transaction usage:

- Increased predictive and preventive controls; reduced detective controls
- Enhanced ability to respond to breaches and security events within their ERP environment
- Increased risk intelligence by correlating isolated security events across the IT landscape
- Improved efficiencies in overall monitoring program by incorporating them into ERP program implementation

Potential Risk Mitigation Steps

- Implement Security Information and Event Monitoring (SIEM) Integration services
- Procure managed services – Security Operation Center (SOC)
Key ERP Trend 2 – Expanding Application Ecosystem

Overview
With the convergence of social, mobile, cloud and information into the application ecosystem; significant user expectation changes regarding how they interact with all technologies including those found in major business applications such as ERP is being created.

Getting to the new world of variably coupled, user-driven ERP will create some major challenges for many organizations.

Impacts
- Increased usage of Connective Technology integrating multiple applications from multiple vendors
- Shift toward Systems of Engagement allowing increased accessibility/agility to employees, vendors, and customers
- Increased exposure of data

Potential Risk Mitigation Steps
- Integrate multiple technologies (e.g., Identity and Access Management (IAM)), Programs and tools
- Focus on personalized security that is dynamic, integrated and seamless for users based on policies and attributes
- Focus on data security requirements (e.g., privacy, PII)
Key ERP Trend 3 – Application Managed Services

Overview

IT organizations are facing a myriad of challenges when supporting their IT infrastructure. These costs tend to grow as the need for business driven real time applications enter a company’s datacenter. Business leaders and customers expect that these systems remain usable, responsive and robust, including the support and maintenance of those systems.

Companies can face an uphill battle when operating a production support model for applications. The support of these applications can consume IT budgets quickly and leave little room for much needed IT projects. Outsourcing of these support services can free up a company's IT department to concentrate on driving business growth and enhancing efficiencies.

Impacts

- Increased ability to support their organizations
- Reduction in the overall cost of maintaining systems and production environments
- Increased ability to concentrate on larger projects

Potential Risk Mitigation Steps

- Take a broad approach to cyber risk on ERP implementations
- Procure Managed Service
Key ERP Trend 4 – Preventing Cyber Attacks

Overview

Attacks are exploiting weaknesses in traditional controls and IT infrastructure, some very destructive. Traditional controls around IT systems are necessary but not adequate – greater emphasis must be placed on preventative controls, rapid detection, and rapid response.

The need for a more integrated supply chain are driving producers to “open up” end of their supply chain to outside vendors and customers. – these connections and relationships must be adequately secured to protect the organization against unauthorized access and protect data when external entities access systems.

Recent cyber attacks highlight the urgency for organizations to contend with ever increasing risks to customer protection, continuity, fiduciary responsibility and operations. Cyber issues lead to brand degradation and change in consumer behavior.

Impacts

- Potential damage to brand position in the marketplace
- Financial loss due to decrease in customer confidence
- Loss of business function or operations due to system downtime
- Potential loss of intellectual property or sensitive data

Potential Risk Mitigation Steps

- Develop security frameworks for the critical cyber infrastructure
- Perform threat assessments for network and infrastructure
- Provide investigation support, readiness support for regulatory compliance (e.g., ITAR/EAR)
- Develop and implement threat response procedures and plans
Next Steps – What can you do to help your organization?

1. Be proactive and talk to the stakeholders of your company’s ERPs and identity two to three Cyber security areas that may be of interest to them and discuss those topics with them.

2. Talk to your company executives about other avenues of cyber security – outside of core ERP. Listen to the challenges they have and the market triggers shared today.

3. Construct a broad approach on addressing and mitigating the Cyber Security Risks.
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.