While most CEOs worry more about a cybersecurity attack than a recession and competitors, most seem to leave security up to the CIO or technology department. As a result, they are showing that they are willing to concede their business’ entire future to the IT department. This executive brief shows CEOs and business leaders at oil, gas, and ethanol manufacturing firms that are particularly vulnerable to attack due to Middle East tensions how they can protect their organization from brand damage, production/supply chain disruptions and revenue loss. Read to gain insights into current threats, evolving technological and operational challenges, and suggestions to help you initiate improvements in your organization.
Recent reports from The Conference Board show that CEOs are more worried about cybersecurity than they are of recession and competitors. They have a valid reason to worry as security breaches overall have increased by 67% over the past five years. Ransomware attacks are growing more than 350% annually, according to Cisco. They estimate businesses will fall victim to ransomware attacks every 14 seconds this year and the number will increase to every 11 seconds by 2021.

These attacks have a cost:
- Baltimore paid more than $18M.
- Atlanta spent more than $20M to recover from an initial $52K ransomware scare.
- Manufacturers have lost between $1M and $10M.

Even though CEOs worry about cybersecurity and the financial implications, they seem to leave it up to the IT department to keep their networks, operations and customers secure. As a result, they demonstrate that they are willing to concede their business’ entire future to the IT department. This thinking has a profound impact on ethanol manufacturers as cyberattacks can create brand damage, supply chain disruption, and loss of revenue. I’ve learned that oil, gas, and ethanol manufacturers are particularly vulnerable to cybersecurity attacks due to Middle East tensions. This year, Iranian hackers targeted thousands of people at more than 200 oil and gas companies across the world, stealing corporate secrets and wiping data from computers. One ethanol manufacturer was able to recover fast after paying a ransom for $54K. But that does not guarantee that the hacker is out of the system and is not going to disrupt back office, production and supply chain operations in the future. Another ethanol manufacturer virtually lost all back-office information and data for more than six months. They waited until attackers penetrated their system rather than taking a predictive, proactive approach that identifies current and future threats ahead of time.

Because of their reactive IT approach, this manufacturer saw impacts on employees, shareholder confidence levels, and back-office operations such as payroll, purchasing, receivables, and budgeting.

The ethanol industry needs to pay attention to the latest hacker threats as their company’s computer networks and their process control systems are vulnerable. All ethanol producers need to do what they can to protect against hackers as I doubt that anyone is truly ready for an attack. Not only do we need to learn how to protect against attacks better, but we need ways to recover from them faster if it should occur.

**LYLE SCHLYER**
President, Calgren Renewable Fuels
After Getting Attacked, Many Ethanol Manufacturers Continue to Take a Tactical, Reactive Approach

Tactical Thinking Traps

After feeling the pain of a cybersecurity threat, many manufacturing CEOs may expand the responsibilities of their IT team and stop relying on 3rd parties for backup. They may compare different plant locations to identify unusual processes and why one site may be more secure.

But they continue to look at a single breached system with a limited view rather than looking at a full overview of the threat landscape. As a result, the focus is only on known threats and exploits, so there is no early warning security system for future threats. By focusing on a single breached system, manufacturers are missing threats that can paralyze the entire connected manufacturing ecosystem.

For example, the WannaCry attack in 2017 infected over 230,000 computers shut down production at Nissan Motor Manufacturing in the UK andRenault2. It led to severe physical and economic losses for the manufacturers.

Here's another reason why it's so important to get a full view of the threat landscape rather than look at a single breached system. The first threat may have only impacted back operations. Next time, they may not be so lucky. You have to be three steps ahead of your attackers who are willing to invest time and effort to target your firm.

Ethanol Manufacturers Are Only Getting Temporary Relief & Temporary Risk Protection

I used to say that there are two types of companies: Those that have were hacked and those that will get hacked. Now, I say there's a third kind: Those that will get hacked again as manufacturers are playing a game of “whack-a-mole” to protect themselves against hackers. They are throwing patches and products at their latest threat.
No matter how many colors and squares, someone will always figure it out

But, a security program is not a group of products that IT purchases. You need a strategic program that is built across people, process, and technology. It starts by identifying where there is compliance, reputational, financial, and operational risk, and it includes:

• Educating your team (as 70% lack a basic understanding of cybersecurity best practices) on the company policy and their responsibility - as well as confirmation that they are following the best practices.

• Documenting workflows and processes and evaluating future initiatives to see what risks are introduced to the environment.

• The development, practice, and execution of incident response and business continuity plan, so disruptions do not last 6+ months.

• Aligning technology with business processes and ensuring controls around the development process and testing process.

• Confirmation that the environment is built to be resilient to attacks.

• Aligning technology with your strategic plan and potential risks

• A plan to reach the appropriate level of maturity at the right time

From a Tactical to Strategic Approach

Step ①
Conduct Risk Assessment
- Compliance Risk
- Operational Risk
- Reputational Risk
- Financial Risk

Step ②
Build Strategic Program
- People
- Process
- Technology

Step ③
Craft Execution Roadmap
- Reach the appropriate level of maturity at the right time – Security is a program not a group of products
- Identify where the jewels are located and address – You can’t protect what you don’t know you have, a risk assessment is critical
To protect the future of the business, ethanol manufacturers need to shift toward a more strategic, aligned business-technology approach, as shown in the chart below:

<table>
<thead>
<tr>
<th><strong>Reactive IT Approach</strong></th>
<th><strong>Aligned Business Technology Approach</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>IT driven</td>
<td>Process driven + IT check</td>
</tr>
<tr>
<td>Focuses on a single breached system (limited view)</td>
<td>Full overview of threat landscape and real-time risk profiling for empowering business decisions</td>
</tr>
<tr>
<td>Focuses on known threats and exploits</td>
<td>Uncovers current threats and yet to be published threats with early warning security systems</td>
</tr>
<tr>
<td>Temporary risk protection with patches</td>
<td>Long term protection</td>
</tr>
<tr>
<td>Engages attackers after penetration leading to 6+ months of disruption</td>
<td>Removes current risk + increases future protection against APT and zero-day attacks</td>
</tr>
<tr>
<td>90% chance of repeat issues</td>
<td>Team training + confirmation of successful systems and programs to reduce future risk</td>
</tr>
<tr>
<td>Limited automation and predictability</td>
<td>Automates security processes and threat hunting with big data and integrated technologies</td>
</tr>
</tbody>
</table>

**CEOs, are you ready to protect your business?**

**next steps**

- Connect with me at JasonOnLinkedIn.com
- SecuringYourTomorrow
- 1.800.549.3312
- jfsmith@isgtech.com