Oil and gas cybersecurity
Penetration testing techniques
Cybersecurity means much more than protecting data. Threats to Operational Technology (OT) systems, can cause production stoppages, a decrease in product quality or even destruction of infrastructure. What do oil and gas executives need to understand about protecting their operational assets from cyber attacks?
Oil and gas company executives today recognize that cybersecurity – the protection of data and intellectual property from organized attacks or individual hackers – is a critical component of risk management. Most oil and gas companies invest significant dollars to manage security on their information networks.

But who is responsible for ensuring that the company’s control systems are safe from cyber attack? Industrial automation and control systems such as SCADA (supervisory control and data acquisition) or DCS (Distributed Control System) – often referred to as Operational Technology (OT) – are used to monitor and control physical processes in the oil and gas industry. Their role is the acquisition of data coming from processes (temperatures, pressures, valve positions, tank levels, chemical compositions, flow demands etc.), human operators and the direct control of electric, mechanical, hydraulic or pneumatic actuators. Is your company making certain that these mission-critical systems are protected properly?

In the past, most OT networks were isolated (air-gapped) from the internet and office networks and operated independently, using proprietary hardware, software and communications protocols. But in recent years, demand for business insight, requirements for remote network access and the spread of hardware and software from traditional IT (e.g., TCP/IP networking, Windows based platforms) caused many oil and gas companies to integrate control systems and their enterprise IT systems. That greater flexibility, however, comes with a very serious risk – it introduces IT vulnerabilities to the world of OT and provides possible access for cyber criminals to infiltrate a network and gain control of OT systems.
Today, there are sophisticated networks of highly skilled “hacktivists” who are not interested in stealing data; they want to create highly visible incidents that embarrass or harm companies involved in the oil and gas industry.
Cyber crime itself has changed in recent years. Today, there are sophisticated networks of highly skilled “hacktivists” who are not interested in stealing data; they want to create highly visible incidents that embarrass or harm companies involved in the oil and gas industry. Taking control of a company’s OT and disrupting operations is one way to do that.

This increased risk requires a significantly more robust approach to OT security than many oil and gas companies are currently taking. Operational technology systems — once the purview of a separate technical department — now demand in-depth, ongoing attention from the chief information officer and their department. And that includes regular reviews of the OT environment and supporting infrastructure, assessments of information flow patterns and usage techniques, and analysis of remote access management tools.

In addition, the security of each component of the network architecture must be tested regularly, from the applications used to operating systems on servers and even the actual field devices that respond to controls.

This type of testing — called “penetration testing” — is done regularly on the information technology side of most companies’ networks. It is designed to mimic the techniques and methodology used by sophisticated attackers who are intent on gaining access to the network. Penetration testing on OT networks is less common, but it works the same way — by identifying and validating gaps in security processes and tools that enable network security professionals to understand how attackers can use those vulnerabilities to alter or disrupt operations. Armed with that knowledge, companies can then take appropriate steps to prevent an attack, just as they currently do in the IT arena.

Ongoing threats and attacks challenge a company’s business assets and the availability of their critical systems and data. EY’s attack and penetration services aim to discover the extent to which an organization is currently vulnerable to exploits that are realistic and probable.

Derived from extensive hands-on experience, our attack and penetration methodology provides a “real life” test of an organization’s exposure to known security threats and vulnerabilities by focusing on exploiting network, application and systems vulnerabilities. Our testing methodology emphasizes manual testing techniques and vulnerability linkage, making EY different from other security vendors and providing more value to you.

Why the hesitancy to test?

Given the importance of penetration testing to OT security, why doesn’t it happen more often? Unlike IT systems, which can be shut down at certain times for testing without major consequences, OT is necessary around the clock, every single day. One reason is financial; even momentary disruptions can result in considerable losses in revenue. More importantly, however, disruptions at facilities such as refineries, petrochemical plants or pipelines, can create major safety and environmental issues. The fear of such a disruption during testing is a major factor in many companies’ hesitancy to test.

Additionally, as OT networks were not networked with business IT networks and, in turn, with the internet, there was little need to test until recently. Thus, many companies have no standard protocol or policy for testing and are reluctant to implement a new program — or unaware that it is necessary.
Oil and gas case study

The client is a major oil company, with upstream, midstream and downstream operations across North America, with sites in Canada and the US, utilizing extensive networks controlled by Operational Technology and Process Control devices.

Objective
The client asked EY to advise on adjusting their OT systems, network architecture and OT security management processes and operations, across their US-based refinery and several Canada-based sites. The client wanted to ensure their systems complied with internally developed formal standards.

Methodology
• EY leveraged its global resources and constructed a team consisting of OT Architects from EY’s Global OT Advisory Center in Poland, Canadian office security auditors and specialized penetration testers from the US.
• A wide range of systems were in scope, including pipeline monitoring and control systems, DCS systems, Safety Information Systems, SCADA systems, RTU systems, PLCs, HVAC systems and UPS systems.
• The compliance project was conducted in two streams:
  • On-site reviews and interviews with technical personnel
  • Penetration testing

How EY helped
• We provided the client with an in-depth view of site compliance with internal OT standards through comprehensive current state assessments.
• Our team identified a series of issues, vulnerabilities and areas of noncompliance within the client’s OT environment and provided a detailed report containing an analysis of all the identified issues, together with their potential consequences.
• All identified issues were rated in terms of residual risk, based on the client’s corporate risk matrix, which made the findings relevant to the client and their board.
• Recommendations were provided that fully explained how the client could proceed toward getting the site’s OT environment from the current state, to the desired state according to the standards used.
Meaningful testing is possible

Despite the issues involved, it is possible to conduct meaningful penetration testing on OT networks, delivering results that can be used to design and implement necessary remediation, without creating operational problems.

To ensure you get value from penetration testing of OT, proper planning is key. We will work closely with your technical personnel and help translate identified vulnerabilities into the risks they pose, to actual physical processes.

EY’s experience of OT testing has shown that communication is essential between the control system support engineers and the individuals conducting the actual test. A multidisciplinary test planning team that includes operations support engineers, consultants experienced in designing and executing OT tests and internal IT security professionals can help promote the exchange of information and ideas so that everyone understands exactly what will take place.

These planning sessions provide opportunities for support engineers to ask questions concerning the testing process, such as the methodology to be used and planned precautions to maintain the operational integrity of production systems. They also allow penetration testers to gain a clear understanding of the implications of testing within an OT environment.

A major focus of pre-test planning should be identifying testing activities that could disrupt critical servers. These activities must be excluded or worked around via alternatives; the health of the testing process must take precedence over any testing objective.

Penetration testing: high-level approach

- Enumerate network
- Interrogate DNS
- Identify hosts

- Scan servers
- Retrieve information
- Assess vulnerabilities

- Validate issues
- Link vulnerabilities
- Perform attacks
- Escalate vulnerabilities

- Collate findings
- Prioritize vulnerabilities
- Highlight suggested actions to be taken

Despite the issues involved, it is possible to conduct meaningful penetration testing on OT networks without creating operational problems, provided that the test itself is properly planned and tightly controlled.
Exploiting vulnerabilities safely

The accuracy of vulnerability identification techniques depends heavily on the specificity and accuracy of the testing process. All potential vulnerabilities that are identified must be examined thoroughly, and the impact of their exploitation should be considered when determining the actual risk to the organization.

If exploiting a potential vulnerability — such as buffer overflows or denial of service activities — the team should carefully consider the appropriateness of performing the test. The gains from better understanding the vulnerability may not outweigh the potential adverse reaction that may result. Whenever possible, these types of activities should be first tested in a development environment.

Understanding social engineering

IT and some OT attacks often involve non-technical methods, also known as social engineering — the art of influencing people into divulging information, performing actions or unintentionally providing unauthorized access through the use of deception, coercion, fear or intimidation.

Social engineering methods include:

• **Phishing** — the use of bait such as fake emails, phone calls or websites, to trick employees into violating an organization’s security policy

• **Physical access** — gaining entrance into the facility itself and using that proximity to access the local network

• **Portable media** — the use of thumb drives and other tools to obtain unauthorized physical access to the network or introduce malicious code through authorized users

Including a social engineering element into a penetration test can help uncover gaps in security policies and procedures and identify weaknesses in personnel awareness training against such attacks. Social engineering also helps to enhance or complement technical activities during a penetration test and more closely resembles the array of activities and methods that would be used by an attacker.
As the boundaries between OT and IT networks continue to blur, and increased convergence leads to higher risk of outside attacks, new security policies and systems must be implemented to ensure the safety of networks that control the oil and gas industry’s facility processes. Penetration testing should be used to identify control gaps and assist with quantifying risks to the OT environment in order to prioritize available security risks and improve the effectiveness of a well-rounded security program.

Key questions to maximize testing

When preparing for a penetration test within an OT environment, consider the following:

1. **What are the goals or expected outcome of the penetration test?** Penetration testing can provide a wide variety of benefits to an organization, such as meeting regulatory compliance, obtaining upper management support for known issues, identifying gaps in state-of-the-art implementations and determining the effectiveness of intrusion detection capabilities. Identifying the goals of the penetration test in advance will help focus the test and provide the best value to your organization.

2. **What are the top threats to the system?** Understanding the motivation for an attack against your control systems will help to identify the most likely attack vectors and assist in discussions of specific scenarios used during the test.

3. **How are your control systems accessible?** Understanding how your control systems are connected (i.e., internet-facing applications, mobile applications, modem or VPN connectivity and business network connections) will help to define an appropriate scope for the penetration test.

4. **Who are the key players that should be involved in the test?** Personnel within the organization that should be involved with the test should be carefully considered. Adequate support should be provided to ensure safety and to make sure the test is meeting the stated objectives. However, excessive involvement from multiple departments may cause confusion with roles for the test or jeopardize the results of testing detection capabilities.

5. **How should testing activities be communicated?** Clearly defined protocols should be created for communicating test activities and results. Procedures should be defined for all roles during the test so that all parties know their individual responsibilities before each phase within the test and actions that should be taken for any contingencies that are determined before testing begins.

6. **Should the testing take place against test or production systems?** Penetration testing on production systems can limit the attack vectors and techniques employed during the test, which may produce results that do not adequately represent the security posture of the systems being tested. Whenever possible, penetration testing should be conducted against test or development systems so that potentially intrusive techniques can be used without jeopardizing safety.

7. **Do test or development systems mirror production?** Penetration testing relies on specific details in the architecture and configuration of the systems being tested. Performing a penetration test against test or development systems will provide a more thorough test; however, the results of the testing may not be valid if the systems being tested do not mirror the systems being used in production.

8. **What information or access should be provided to the tester?** Black box (zero knowledge) and white box (full knowledge) testing have different advantages and disadvantages depending on the goals of the assessment. In general, black box testing should be used to identify the access an outside attacker could gain without pre-existing knowledge or access to the system; however, it may be beneficial to provide additional access or knowledge at certain phases during the test to make sure test objectives are met within the time allocated for the test.
How EY can help

EY offers a broad range of threat and vulnerability services – from attack and penetration testing to security program management – enabled through our Advanced Security Centers (ASCs). Our services are designed to bring you the best answer to solving your threat concerns. After an initial discussion, we will suggest one or more of the following assessments to evaluate your current environment and allow you to be in a better position to win in the perennial fight against IT risks.

Our ASCs perform attack and penetration assessments of your network infrastructure to attempt to identify vulnerabilities from various risk perspectives, including the true outsider, malicious insider and third parties with limited access: each of these assessments follow a similar approach that includes discovery, vulnerability identification and exploitation phases. With your permission and coordination, we attempt to penetrate the identified systems using an agreed controlled testing approach and then exploit the identified vulnerabilities.

Our infrastructure assessment services include:

• External network attack and penetration
• Internal network attack and penetration
• Wireless network attack and penetration
• Dial-up assessment
• Cloud infrastructure attack and penetration
• OT network assessments
• Mobile device and infrastructure assessments

The results of these assessments will enable you to take steps to eliminate the identified risks.

Case in point

An oil and gas company didn't believe it had any data leakage issues. However, after an attack a peer experienced, the company decided to hire an outside provider to ensure that its information was secure.

On day two of EY’s assessment, our team discovered that a foreign jurisdiction was accessing sensitive information about proprietary intellectual property and sending it overseas. Our client had no customers in that jurisdiction and no good business reason for the information to be flowing in that direction.

Based on the results, which surprised the board and the audit committee, the organization completely rethought its approach to handling information – how to protect information and enable its use.
Conclusion

For oil and gas executives, the first step in protecting the company’s critical operational assets is recognizing and understanding the very real threat that OT networks face from cyber criminals. These attacks are part of an ongoing attempt by individuals and groups around the world — in some cases funded by other governments or government entities and nation-states — to disrupt the oil and gas marketplace and damage the financial standing of companies.

No company is immune from cyber attacks. Outside groups are constantly probing oil and gas company networks, looking for weaknesses that can be exploited. The good news is that penetration testing, when done correctly, can provide the same benefits to operations control networks and applications as it does for IT.

EY can assist oil and gas companies in protecting their OT networks and related operations assets through a systematic, well-structured testing process that identifies and prioritizes vulnerabilities. From there, we work with your internal experts to develop proper policies and implement appropriate hardware/software tools so that your OT network is secure — and remains that way.
The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

How EY’s Global Oil & Gas Center can help your business
The oil and gas sector is constantly changing. Increasingly uncertain energy policies, geopolitical complexities, cost management and climate change all present significant challenges. EY’s Global Oil & Gas Center supports a global practice of more than 9,600 oil and gas professionals with extensive experience in providing assurance, tax, transaction and advisory services across the upstream, midstream, downstream and oilfield service sub-sectors. The Center works to anticipate market trends, execute the mobility of our global resources and articulate points of view on relevant key sector issues. With our deep sector focus, we can help your organization drive down costs and compete more effectively.

© 2014 EYGM Limited.
All Rights Reserved.

SCORE No. DW0307
WR No. 1405-1259913
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/oilandgas