AGENDA
A Financial Times Service

Opinion

Managing Insider Threats Is a Key Component to Cyber Security

June 13, 2016

Thomas Kennedy is the chairman and CEO of **Raytheon**.

Most directors recognize the growing importance of cyber security, but not enough boards take the right steps to ensure an effective risk management process is in place, particularly when it applies to insider threats.

Insider threats may be overlooked, but they are critical.

These threats can take the form of a malicious employee downloading sensitive intellectual property for a competitor or an unhappy employee destroying data before quitting.

An inside threat can also simply be a rule bender who intentionally bypasses a defensive system or policy they find inconvenient, such as by e-mailing sensitive documents home to work on over the weekend.

Companies fail to act on the risk of an insider threat at their own peril, usually for one of two reasons: They may deny the problem exists or find it too overwhelming to tackle. Either way, the result is often inaction, resulting in unmitigated risk to a company's personal employee information, trade secrets, internal communications, business intelligence and customer data.

Boards can play a role in addressing insider threats by instructing management to take action in the following essential areas:

1. Policy

Defining acceptable use of company resources is the first and most important step, including defining which activities are permitted on your network and which are not.

Setting clear policies does not mean you make them so restrictive that you disrupt the business or drive off tech-savvy employees, but it does mean drawing very clear boundaries for employee behavior that you can train to and monitor. This behavior will likely be adhered to, since employees generally want to do the right thing. Those who don't will stand out if the rules are clear.

2. Employee Education

Ensure that your company educates employees throughout their careers. Good training brings to life the dangers of bending rules and how to be alert for malicious insiders. Pairing insider training with training on external threats will make your employees part of the solution, not part of the problem.

3. Access Controls

Not every employee needs access to every piece of data, so segment your networks and restrict privileges to ensure that employees can access only files and applications they need. For example, your accounting

department probably has no need to access engineering drawings. And employees in one country may not be legally allowed to access customer data from another country. Such controls can be enforced at the network level by encrypting data at rest and using firewalls to physically prevent traffic from flowing between areas. You can also assign specific roles to employees with identity management or data-labeling tools. The larger the company, the more likely it will need all of these controls.

4. Monitoring

Your company must measure actual, not intended, results of security efforts — you must know when you fail. Effective monitoring programs combine technology with aggressive operational processes to monitor for unusual employee network behavior. The technology detects suspected violations. The operational processes and skilled staff make sense of the data. Failure to balance technology and operations never ends well.

5. Auditing

Where monitoring is the real-time detection of undesired activity, auditing is the long-term, deliberate evaluation of the underlying processes and policies. Audits reveal gaps and blind spots in your insider threat program. One of the highest payoffs of an audit is to highlight privileged individuals and functions exempted from security controls or monitoring. Exemptions are not necessarily wrong, but all too often those areas are where problems occur. Audits ensure such risks are taken with eyes wide open.

The bottom line is that the days are gone when boards could assume someone was handling cyber security without identifying who exactly that “someone” was and what they were doing. A matter as serious as the insider threat requires your direct involvement. Nothing less than the future of the company is at stake.