Power up your retail security strategy
Information protection imperative to customer trust

Today’s customers have high expectations. With so many choices and ways to buy, customers know that if they don’t find exactly what they want from one retailer, they can easily go elsewhere. Successful retailers already are engaging customers through “omnichannel” shopping – a mash-up of online and physical experiences. Retailers are adopting an omni-channel approach – an integrated strategy of delivering a seamless, consistent customer experience using every possible touch point, including mobile devices, retail websites, brick-and-mortar stores, TV, catalog, and direct mail.

Facing the Reality
Regulatory and compliance requirements, alongside the need for companies to protect themselves from brand damage and revenue losses, drive the retailer to employ better protection against security threats. All-in-all, organizations remain vulnerable and need to do more to deal with the wide range of security threats.

Understand the Threat Vectors
Data breaches pose a real risk to customer confidence and company profits; but are they really so common? Retail organizations are among the top five targeted industries. Why? Because they process massive amounts of financial data, and many do so from multiple stores across multiple states every single day. As a result, there are hundreds of potential access points for an attacker. It is safe to assume, at any given moment, that every major retailer in the U.S. is under attack; even if 99 percent of these attacks are deflected, the threat is real – and continuous. It is also worth noting that security is not the same thing as compliance. Since Payment Card Industry Data Security Standards (PCI DSS) compliance can be a long and complex procedure, it is often easy to equate the process with effective security. Compliance is adherence to government or industry standards or regulations; security is the protection of the information contained in the data.

Prioritize your Business Objectives and Set your Risk Tolerance
Striking a balance between protecting data assets and enabling productive, innovative workplaces has challenged security professionals for decades. The truth is that there is no such thing as being 100 percent secure. Difficult decisions need to be made around the different levels of protection needed for different parts of the business.

Information a Critical Asset
Before assessing cybersecurity solutions, a company must identify its most critical data. This data can be anything from financial information to consumer or client information. It is important to control and monitor who has access to that valuable and vulnerable information so that no one except authorized individuals can obtain it.

Executive Buy-in and Team Effort
Engage everyone in the security effort. To increase cybersecurity effectiveness, make sure everyone is involved. Do not operate in silos. Provide employees with regular updates, training and education on how they can safeguard data.

Focus on Application Security
Businesses handling customer financial information have a responsibility to improve software quality and reduce the operational risk of their applications – not only to protect their businesses, but ultimately to protect their customers. With more retailers and customers using these applications, ensuring adequate security across multiple platforms is critical to mitigate risks and to avoid devastating data breaches. A data breach can have a deep impact to the bottom line; but it can also undermine customer confidence, damage your brand and reputation, and reduce customer loyalty.

Invest in Threat Management
Today’s cyber world is plagued with increasing security risks. The attacks are becoming more frequent, more complex, and more dangerous. It may seem an overwhelming task to try and protect against every threat. In fact, the reality is that no environment can be fully immune to attack. Therefore, the most important part of a security program is a robust monitoring, detection, and response system. However, in today’s complex world where everything is mobile and users have access to a diverse set of apps, devices, storage, and network connectivity, threat management remains a difficult task. Among the challenges are the ability to see enough data to detect an issue and to distill large amounts of data down to a set of meaningful and actionable alerts.

To learn more about AT&T Security Consulting, visit www.att.com/security-consulting or have us contact you.
Have a Trained and Tested Incident Response Team
Despite these repeated warnings, many executives still don’t take cyber threats and data breach risks seriously enough. They underestimate how frequently such incidents arise, typically assuming that it will not happen to their business. When incidents do happen, it is common for them to try to sweep them under the carpet in an attempt to preserve the organization’s reputation and consumers’ trust.

Securing Point of Sale
Threats to point-of-sale (POS) systems are not new, but there has been considerable media attention related to recent large-scale breaches of cardholder data and other personal information from retailers’ systems. Reviewing the tactics employed in these attacks may help organizations identify ways to augment existing threat models and enhance security design and response efforts. All security measures can potentially be circumvented, but organizations can strengthen their security profiles by layering defenses and by understanding normal and appropriate activity in their networks versus potentially anomalous activity worth immediate investigation.

Protecting your data, reputation and business
Leading retail organizations take a more strategic approach to security to respond to the new challenges.

• Understand the organization’s key assets and appetite for risk. Align business and IT leaders on the prioritization of digital assets based on value and risk to the organization to ensure the proper design of technology, processes and supporting resources. For example, customer data, point-of-sale and order management systems are a higher priority while marketing and promotion systems may be lower.

• Identify the security risks and gaps. Assess current security capabilities and determine the likelihood of experiencing known and emerging risks. Business and IT leaders should then align on the gaps and the estimated mitigation costs.

• Define the cybersecurity strategy. Based on a thorough understanding of the organization’s security priorities and potential gaps, IT should create comprehensive technology, process and organizational designs and blueprints with strategic and operational elements that protect digital assets.

• Emphasize gaps, priorities and strategy to the CEO and board. Leadership should know about the security-related risks and gaps they face so they can understand the importance of the investments required.

• Engage recognized security specialists. As the threat landscape expands and attacks become more sophisticated, organizations should work closely with firms that can provide ongoing services to diagnose, redesign and monitor their cybersecurity.

Develop an Action Plan: Use a Security Framework

Identify
- Asset Management
- Business Environment

Protect
- Access Control
- Training
- Data Security/Management
- Incident Response Plan
- Protective Technology

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Detect
- Anomalies
- Security Monitoring
- Processes

Recover
- Recovery Planning
- Improvements
- Communication

Final Thoughts
Focus has been on the retail sector due to recent well publicized data breaches, but a similar breach could happen in almost any business. An attacker may pursue credit card data, healthcare records or intellectual property. It is essential to implement a holistic security strategy plan to protect your organization’s assets. This starts with mapping out all possible internal and external threat scenarios in your environment and using a third-party security expert to assess your infrastructure.

For more information contact an AT&T Representative or visit www.att.com/security-consulting.
Have a Trained and Tested Incident Response Team
Despite these repeated warnings, many executives still don’t take cyber threats and data breach risks seriously enough. They underestimate how frequently such incidents arise, typically assuming that it will not happen to their business. When incidents do happen, it is common for them to try to sweep them under the carpet in an attempt to preserve the organization’s reputation and consumers’ trust.

Securing Point of Sale
Threats to point-of-sale (POS) systems are not new, but there has been considerable media attention related to recent large-scale breaches of cardholder data and other personal information from retailers’ systems. Reviewing the tactics employed in these attacks may help organizations identify ways to augment existing threat models and enhance security design and response efforts. All security measures can potentially be circumvented, but organizations can strengthen their security profiles by layering defenses and by understanding normal and appropriate activity in their networks versus potentially anomalous activity worth immediate investigation.

Protecting your data, reputation and business
Leading retail organizations take a more strategic approach to security to respond to the new challenges.

• Understand the organization’s key assets and appetite for risk. Align business and IT leaders on the prioritization of digital assets based on value and risk to the organization to ensure the proper design of technology, processes and supporting resources. For example, customer data, point-of-sale and order management systems are a higher priority while marketing and promotion systems may be lower.

• Identify the security risks and gaps. Assess current security capabilities and determine the likelihood of experiencing known and emerging risks. Business and IT leaders should then align on the gaps and the estimated mitigation costs.

• Define the cybersecurity strategy. Based on a thorough understanding of the organization’s security priorities and potential gaps, IT should create comprehensive technology, process and organizational designs and blueprints with strategic and operational elements that protect digital assets.

• Emphasize gaps, priorities and strategy to the CEO and board. Leadership should know about the security-related risks and gaps they face so they can understand the importance of the investments required.

• Engage recognized security specialists. As the threat landscape expands and attacks become more sophisticated, organizations should work closely with firms that can provide ongoing services to diagnose, redesign and monitor their cybersecurity.

Final Thoughts
Focus has been on the retail sector due to recent well publicized data breaches, but a similar breach could happen in almost any business. An attacker may pursue credit card data, healthcare records or intellectual property. It is essential to implement a holistic security strategy plan to protect your organization’s assets. This starts with mapping out all possible internal and external threat scenarios in your environment and using a third-party security expert to assess your infrastructure.

Develop an Action Plan: Use a Security Framework

Identify
- Asset Management
- Business Environment

Protect
- Access Control
- Training
- Data Security/Management
- Incident Response Plan
- Protective Technology

Respond
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

Detect
- Anomalies
- Security Monitoring
- Processes

Recover
- Recovery Planning
- Improvements
- Communication

Share this with your peers

For more information contact an AT&T Representative or visit www.att.com/security-consulting.