As cloud security threat levels continue to shift, the defenses that organizations employ must also adapt to meet the crucial challenges ahead.

Introduction
Cloud computing is profoundly changing the IT landscape. Unfortunately, some of these changes have created new security challenges. While IT departments have been focusing on securing their on-site computing for decades, working with outside cloud computing providers has exposed new vulnerabilities that must be addressed both internally and by the cloud computing providers.

The security threats associated with cloud computing are continuing to evolve, while the perceived and actual level of certain security threats has also changed over the last several years. In this paper we’ll examine some of the current major cloud security threats, how and why the importance of those threats has changed as well as the perceived versus actual threat levels. The paper will then take a closer look at two leading cloud threats — phishing and denial-of-service (DoS) attacks.
The changing cloud threat landscape
Over the last several years, the threats facing cloud computing have gained increasing coverage in the media, while the list of top threats has remained relatively unchanged. In 2010, the Cloud Security Alliance polled cloud security experts to determine what they viewed as the top threats and to prioritize the list based on the perceived importance of these threats. In February 2013, the same organization published a new version of the report, titled “The Notorious Nine – Cloud Computing Top Threats in 2013”. The table below lists the 2010 and 2013 results:

<table>
<thead>
<tr>
<th>Cloud security threat</th>
<th>2010 rank</th>
<th>2013 rank</th>
<th>Change from 2010 to 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data breaches</td>
<td>5</td>
<td>1</td>
<td>+4</td>
</tr>
<tr>
<td>Data loss</td>
<td>5</td>
<td>2</td>
<td>+3</td>
</tr>
<tr>
<td>Account or service traffic hijacking</td>
<td>6</td>
<td>3</td>
<td>+3</td>
</tr>
<tr>
<td>Insecure interfaces and APIs</td>
<td>2</td>
<td>4</td>
<td>-4</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Not on list</td>
<td>5</td>
<td>+ at least 4</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>3</td>
<td>6</td>
<td>-3</td>
</tr>
<tr>
<td>Abuse of cloud services</td>
<td>1</td>
<td>7</td>
<td>-6</td>
</tr>
<tr>
<td>Insufficient due diligence</td>
<td>7</td>
<td>8</td>
<td>-1</td>
</tr>
<tr>
<td>Shared technology vulnerabilities</td>
<td>4</td>
<td>9</td>
<td>-5</td>
</tr>
</tbody>
</table>

Table 1: Top cloud computing threats in 2013.

Changing tactics used by attackers and changing tools to combat attacks
Despite what you think about the people and organizations attacking your IT investments, you must admit they are adaptable. As known cloud security vulnerabilities are addressed by the industry, attackers are quick to identify and exploit new ones. Even when cloud-based systems are locked up tight, targeted phishing attacks or malicious individuals employed by the target can yield the security credentials needed to penetrate seemingly secure systems. And when broad attacks aren’t working well, the attackers turn their focus to developing malware designed specifically to attack a particular target.

According to Dell Security Expert Mark Wood: “Fifteen years ago, DDoS attacks never happened. Now they’re a top ten threat. Phishing attacks are new within the last decade and now they’re a top vector for unauthorized access. Attackers are now using custom malware written for a specific target. The adversary continues to develop new ways to compromise data confidentiality, data integrity, or system availability, which is why the Notorious Nine threats continue to evolve.”

To stay ahead of threats, IT security providers have to stay on top of their game and continue to eliminate vulnerabilities, develop new security protocols and utilize every method in their defense arsenals to thwart the attackers.

The greatest opportunities for cloud security threat mitigation today
In order to significantly reduce cloud security threats, it’s important to focus on the threats that have increased most over the last several years. According to the Notorious Nine report, these threats are:
- Data breaches
- Data loss
- Account or service traffic hijacking (including phishing)
- Denial of service

Dell cloud security experts report that phishing and denial-of-service (DoS) attacks are some of the most common security requests they receive.

In the remainder of this paper we will take a more detailed look at these two threats.

Threat mitigation
“The market is demanding flexible and varied cloud solutions, based on specific needs and uses. Security must, therefore, be tailored to the specific use and anticipate the ever-changing threat landscape.” — Jeremy Ford, executive director, Cloud Services, Infrastructure and Cloud Computing, Dell Inc.

The tools and techniques used to mitigate cloud security threats must evolve quickly in order to keep up with the changing attack tactics. This section will examine some of the techniques used to mitigate phishing attacks and denial-of-service attacks.

Phishing attack mitigation
Phishing attacks are sophisticated scams designed to trick victims into divulging sensitive data, like account numbers and authentication credentials. They may be
targeted at your users or your customers. All it takes is one individual to be fooled by a phishing email and they can end up providing sensitive information or downloading malware.

Phishing emails often link to websites designed to look like a legitimate site, however, the links on the site download malware or entice the visitor to provide their personal and/or financial information. Because the fraudulent websites are outside of your network — often in other countries — shutting them down and ending the threat to your business requires strong countermeasures and education of your customer and users.

If your company owns one or more well-known brands, you may find that phishers have created emails and websites that appear to be associated with your company/brand/products. Stopping these emails and getting the fraudulent sites taken down can be challenging and often requires skills that are outside the normal skills of your security team. You may want to consider working with an outside firm that has experience successfully combating phishing attacks. Some of the suggested techniques to combat phishing include:
- Create a response plan
- Implement countermeasures
- Report the incident
- Take down the phishing websites
- Post incident analysis and reporting

It is also important to educate your internal users and customers about phishing threats and how they can help minimize their impact. As a general rule, your customers and employees need to be careful about providing sensitive information over the Internet. As the leading provider of information on how to mitigate phishing attacks, the Anti-Phishing Working Group offers lists of suggestions to share with your users and customers. You can also reach them by phone.

If your company or organization may be on the receiving end of phishing attacks, the following list includes some of their high-level recommendations:
- Be suspicious of any email with urgent requests for personal information — financial or otherwise.
- Don’t click the links in an email, instant message or chat if you suspect the message might not be authentic or you don’t know the sender or user’s handle.
- Avoid filling out forms in email messages that ask for personal information.
- Always ensure that you’re using a secure website when submitting credit card or other sensitive information via your web browser.
- Remember, not all scam URLs will appear as “https” and may display the security lock, so it is important to look at the address line, too. Were you directed to PayPal? Does the address line display something different like: hxpx://gotyouscammed.com/paypal/login.htm? Be aware of where you are going.

Denial-of-service threat mitigation
Denial-of-service (DoS) attacks attempt to overwhelm your computing infrastructure in order to make your services/sites unusable. For sites that generate a lot of revenue, a DoS attack can quickly cause financial harm to an organization. One of the most commonly used types of DoS attacks are distributed denial-of-service (DDoS) attacks. DDoS attacks are characterized by attacks coming from multiple computers. With a regular DoS attack, it is often possible to block the single attacker and restore services. A DDoS attack, however, could involve hundreds or thousands of computers, including computers that have been infiltrated by malware specifically designed to be used in DDoS attacks.

DDoS attacks are increasingly being used to distract a security group so the attackers can launch other types of

“Phishing attacks are new within the last decade and now they’re a top vector for unauthorized access…”
Mark Wood
Dell Security Expert
Dell Inc.
attacks at the same time. For instance, in 2011 a coordinated DDoS attack was launched against Sony. While Sony’s security team was battling the attack, no one noticed that the attackers successfully breached over 101 million Sony PlayStation user accounts.

Like phishing attacks, combating DoS attacks requires a coordinated, sophisticated approach. Experts recommend a number of steps:
- Plan ahead — before you are attacked
- Identify and secure parts of your network that are the “weak links” (easily overwhelmed by a DoS attack)
- Design your infrastructure so it can easily handle large spikes in activity
- Actively monitor your network traffic
- Prepare for multiple types of DoS attacks including packet flooding, application-layer attacks and attacks that combine multiple types
- Don’t go it alone — consult experts and involve your internet service provider and/or cloud provider as they can often help mitigate DoS attacks
- Have countermeasures in place that can quickly respond to an attack

An overview of cloud security offerings from Dell

Dell provides a robust suite of cloud security offerings that utilize the latest technologies and services to mitigate threats. This section provides a brief overview of each offering.

Dell Phishing Mitigation Services

Dell SecureWorks provides the following anti-phishing services to help companies before and after a phishing incident occurs:
- Phishing Incident Preparation
- Phishing Incident Response Plan
- Phishing Incident Response
- Countermeasures and Coordination
- Interim Reporting
- Post Incident Analysis and Management Report
- Phishing Takedown

Phishing Incident Preparation

Phishing Incident Response Plan

Having a Computer Security Incident Response Plan (CSIRP) immediately following an attack is critical. This plan provides details of response procedures, processes, responsibilities and points of contact. The CSIRP also outlines roles and responsibilities, along with steps for communicating time-sensitive phishing-related information. The latest threat intelligence on actors and tradecraft should be included in this plan.

Phishing Incident Response

Dell SecureWorks professionals are available to respond to incidents 24 hours a day, seven days a week, 365 days a year. The team begins by gathering details of the attack including:
- Networking analysis: Traceroute, DNS lookups, ARIN searches, OS fingerprinting, scanning, system enumeration, footprinting
- Application analysis: Website code reviews, email analysis, server configuration
- Research: IRC, USENET, websites
- Propagation methodologies and magnitudes
- Severity assessment
- Log review: Web logs, server logs, firewall logs

Countermeasures and Coordination

Dell SecureWorks will recommend, coordinate, manage and facilitate an appropriate selection of countermeasures. Dell works with key anti-phishing and security organizations including FIRST (the Forum of Incident Response and Security Teams; Dell SecureWorks is a full member), the United States FBI and Secret Service, CERT (Computer Emergency Readiness Team), and the Anti-Phishing Working Group. Dell SecureWorks also works with local and foreign internet service providers, foreign law enforcement and vendors.
Interim Reporting
Dell SecureWorks will provide interim reports to keep key personnel and other involved parties apprised of the response.

Post Incident Analysis and Management Report
After a major incident has been resolved, Dell SecureWorks will review and document the effectiveness of your incident handling process and identify needed improvements to existing security controls and practices. Dell SecureWorks will also produce a post-incident report with an executive summary that discusses the impact to your organization, your business and your customers.

Phishing Takedown
If your organization is being targeted by phishing attacks, Dell SecureWorks is available 24x7x365 to recommend, coordinate, manage and facilitate an appropriate selection of countermeasures including removal of the phishing site.

Denial-of-Service Mitigation Services
The Dell SecureWorks Incident Response and Digital Forensics team can help your organization build an incident response plan for denial-of-service (DoS) attacks that maps to your environment and staffing model. Our expertise and experience responding to DoS attacks will provide insight for best practices, as well as common pitfalls. The Denial-of-Service Preparedness Assessment includes several options designed to help you understand your organization’s risk exposure and ability to withstand DoS attacks. It will also ensure that you have a tested response methodology in place. These proactive steps can help limit the impact of future denial of service and distributed denial-of-service attacks on your organization.

With Dell SecureWorks, you can:
- Update your computer security incident response plan (CSIRP) with response procedures for Dos and DDoS attacks
- Learn strategies to effectively deal with DoS and DDoS attacks of various magnitudes
- Establish roles, responsibilities and processes needed to effectively respond
- Implement network tools to identify when a DoS or DDoS attack is happening and determine its source
- Learn how you can improve your architecture to strengthen resistance to a DoS and DDoS attack

Illustration 1: Map your incident response plan to limit the impact of future denial-of-service and distributed denial-of-service attacks on your organization.

“The market is demanding flexible and varied cloud solutions, based on specific needs and uses. Security must, therefore, be tailored to the specific use and anticipate the ever-changing threat landscape.”

Jeremy Ford
Executive director, Cloud Services
Infrastructure & Cloud Computing
Dell Inc.

Heightened preparedness
Infrastructure stress testing
DoS tabletop exercise
Instrumentation capabilities review
Preparedness assessment
Conclusion

No matter what cloud computing security threats your organization faces, Dell has the services and tools to help you mitigate those threats.

In addition to our own security experts, Dell partners with best-in-class security providers and is committed to industry-leading security through SecureWorks — world-class information and IT security services that help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Next steps
Now is the time to find out how Dell SecureWorks can help secure your cloud computing projects and infrastructure. Call 877-838-7947 (UK +44 131 260 3044) today to begin the discussion.

For more information about any of our other service offerings, please visit Dell.com/services or contact your Dell representative.