To: Information Security Coordinators
    Information Technology Coordinating Council
    Technology Leaders
From: David Kovarik
Subject: Monthly Security Report for November, 2010
Date: December 15, 2010

During the month of November 2010, we experienced 166 Security Events including 27 Security Incidents, all of Low Severity. For November 2009, we had a total of 135 Events.

<table>
<thead>
<tr>
<th>Security Incidents</th>
<th>NUSA Notifications</th>
<th>Copyright Violations</th>
<th>Total Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 2010</td>
<td>27</td>
<td>94</td>
<td>45</td>
</tr>
<tr>
<td>Nov 2009</td>
<td>17</td>
<td>65</td>
<td>53</td>
</tr>
</tbody>
</table>

The November Events are separated into the following categories:

<table>
<thead>
<tr>
<th>NetIDs</th>
<th>IP Addresses</th>
<th>Total Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incidents</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>NUSA Notifications</td>
<td>0</td>
<td>94</td>
</tr>
<tr>
<td>Copyright Violations</td>
<td>31</td>
<td>14</td>
</tr>
<tr>
<td>Total Events</td>
<td>43</td>
<td>123</td>
</tr>
</tbody>
</table>

**Vulnerability Assessments**

- Quarterly Data Center Web Scans
- The Graduate School (QualysGuard)
- Monthly network assessment for Proteomics Center of Excellence
- McCormick/Computer Science (Google Hack)

**Service Provider Security Assessment**

- Buckeye Innovations
Table and Category Descriptions

Security Incidents
Actual compromise of a system or application; includes investigations conducted as a result of a suspected or actual incident.

Security Events
The combination of Security Incidents (as defined above) and the following:
Copyright violations
Events that are usually indicated by receipt of external notification that one of our hosts is being used to distribute copyrighted material in violation of the DMCA. Often these hosts are running various forms of Peer to Peer networking software.
NUSA notifications
Events indicated by our remote vulnerability scanning software that detected a potential security problem (vulnerability) with the host. We put this information into NUSA to notify the system administrator so that the problem may be addressed before it is exploited.

NetIDs
Events where a specific Northwestern NetID is identified and typically occurring on either the wireless or wireless networks. Events include instances where a compromise of the NetID may have occurred, usually as a result of phishing or other social engineering activities.

IP Addresses
Events where a NetID might not be able to be determined or is not directly involved, e.g., a compromised host.
## Summary Report of Security Incidents

<table>
<thead>
<tr>
<th>Action / Recommendation</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NU Policy and Illinois Law.</td>
<td>3</td>
<td>The computer was re-built and re-issued, no public announcement was made. As all individuals were notified and sent notification letters, all individuals were reported by the department.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On March 3, 2010 it was reported by a department that a personal computer had been compromised. A spreadsheet containing personal health information had potentially been exposed to unauthorized access.</td>
</tr>
</tbody>
</table>

Severity 2 and 3, November 2009 - November 2010
begins to look as though you're accessing your personal information being accessed, harvested, and used to compromise your account. However, it is likely that your account number, account number or password, billings and even personally identifiable information (PII) such as credit card number, social security number, or account number from a well-known organization and ask for your personal information. These are usually external notifications we receive indicating that one or more hosts is being used to distribute network software.

vinfectability has a high probability of compromise.

The notification is placed into NSN, and notification sent to the NNSA to address the problem.

Indicates that our remote vulnerability scanning software detected a potential security problem with the host.

This host is being used to distribute various types of bulk email. Other these hosts are used with a backdoor that allows password to use the host to send e-mail of their choice.

These hosts are used to attack other networks.

The host has been determined to be executing commandos of the connecting host. Other these hosts are used with a server to transfer files of various types and often illegal content.

This host was detected as an FTP server, typical of many types of infections. The FTP server was subjected to a malware infection and its attempt to propagate.

This host was detected performing outbound scans on various TCP ports. This condition is often indicative of malicious activity.

Security Incident: Severity 1 (Low)
Security Events by Month (by Category)

2009 - 2010

November December January February March April May June July August September October November

Incidents
CopyRight Violations
NUSA Notifications

Security Events by Month (by Category)
Security Events by Calendar Year by Category

- Incidents
- Copyright Violations
- NUSA Notifications

Year: 2005 - 2010

- 2010: 1100
- 2009: 1041
- 2008: 953
- 2007: 1136
- 2006: 123
- 2005: 938

- 2010: 403
- 2009: 678
- 2008: 762
- 2007: 123
- 2006: 88
- 2005: 88