The next big real estate challenge: Cybersecurity and smart buildings

Let's talk about an opportunity.
Gain an understanding of:

> Current use of Internet of Things (IoT) technologies in development
> Understand the benefits and risks of connecting your real estate assets
> Learn about precautionary measures you can take in early development stages
Thinking “inside” the box

- Parking assistance
- Air quality sensors
- Smart temperature gauges
- Smart windows
- Human powered gyms
- Rainwater toilet water systems
- Smart elevators
- Smart lighting
- Activity sensors
Consequences

> Physical damage to equipment or infrastructure
> Theft of high value property
> Loss of revenue
> Accidents/bodily injury or death
> HVAC shutdown/manipulation
> Door locks disabled
> Disabling of physical intrusion detection systems
> Loss of building lighting
> Data center thermal overloads
> Significant loss of revenue
> Loss of customer confidence/contracts
> Higher insurance premiums
Expanding attack surface

Convergence of (IT) and (OT)

Lions attack the slowest gazelles

It’s not if, but when

Impact is on tenant as well as owner

Extortion fancies urgency
Direct to consumer crime
>
> Mostly email based
> Social engineering
> Reconnaissance
> You don’t know it’s happening

Yes, YOUR buildings are a target

“Amateurs go after technology, professionals go after humans.”
- Bruce Schneier, 2000
Types of phishing attacks

> **Phishing** – An email that masquerades as a trustworthy entity in an electronic communication.

> **Spear Phishing** - an email that appears to be from an individual or business that you know, however it is not.

> **Whaling** - personalized phishing or spear phishing aimed at senior executives in an organization.

> **Payloads:**
> - Credential grabbing (Executive impersonations)
> - Malicious links
> - Malware (e.g. Ransomware)
From: Chase Bank <xpw@cendanatour.com>
Date: Thu, Mar 16, 2017 at 8:48 PM
Subject: Bill Pay Reminder #862760742
To: <al.sweeny@gmail.com>

Hi,

This is the reminder you asked for when a payment to GAS UTILITIES may be due:

Recipient: GAS UTILITIES
Account: xxxxxxxxxxxxxx483
Amount: $2219.00
Deliver By Date: 03/26/2017

No action is needed if you already had make a payment.

To view your bill or pay it:

Check your bill.

Thanks for using Chase Bank BillPay.

To stop getting reminders like this, sign in to Chase Bank BillPay and change your reminder settings for GAS UTILITIES.

Do not reply to the message.
Message ID: TLM0372 WOL
Facilities reconnaissance
# Facilities Enumeration

### General Information

<table>
<thead>
<tr>
<th><strong>Garbage Day:</strong></th>
<th>Monday</th>
</tr>
</thead>
<tbody>
<tr>
<td>* &amp; <strong>Recycle Day:</strong></td>
<td>Monday, 11-28-1999</td>
</tr>
<tr>
<td>1999 Fall Leaf Collection Dates:</td>
<td>October 10-14, October 24-28, November 7-11</td>
</tr>
<tr>
<td>Water Source:</td>
<td>Lamar County</td>
</tr>
<tr>
<td>Sanitary District:</td>
<td>Lamar County</td>
</tr>
<tr>
<td>School District:</td>
<td>Blossom</td>
</tr>
<tr>
<td>Elementary School:</td>
<td>Roxton</td>
</tr>
<tr>
<td>Middle School:</td>
<td>Toco</td>
</tr>
<tr>
<td>High School:</td>
<td>Reno</td>
</tr>
<tr>
<td>Fire Station Number:</td>
<td>3</td>
</tr>
</tbody>
</table>

Unlocked dumpster
By reviewing historical images available via Google Earth, it is clear that this company has updated their HVAC system recently. Baker Tilly noted an area of the building that didn’t have any evidence of a heating or cooling system there as of May 2011. In April of 2014, there is one heating or cooling unit that can be plainly seen. As of Google Earth’s most recent images, there are multiple heating and cooling units that are visible. The older units on the other side of the building are still present during this time frame. This creates two interesting scenarios:

> A new system that is likely network connected

> An old system that could potentially be easily exploited.
One of the most prolific breaches in recent history, which affected the retailer Target, all stemmed from stealing credentials used by the company that had recently installed a new HVAC system at a Target store.
"port:554+has_screenshot:true"
<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthenticated protocols</td>
<td>• Identify all unauthenticated protocols</td>
</tr>
<tr>
<td></td>
<td>• Assess whether current equipment can support authentication options.</td>
</tr>
<tr>
<td></td>
<td>• Implement authentication options where feasible</td>
</tr>
<tr>
<td></td>
<td>• Implement bump-in-the-wire authentication on legacy</td>
</tr>
<tr>
<td>Outdated hardware</td>
<td>• Consider upgrades for older devices that have network connectivity and support critical process control functions</td>
</tr>
<tr>
<td></td>
<td>• Implement firewall rules to minimize network connectivity of devices with outdated hardware</td>
</tr>
<tr>
<td>Weak user authentication</td>
<td>• Match internal device inventory against list of devices known to have hard-coded passwords</td>
</tr>
<tr>
<td></td>
<td>• Monitor device logs and network traffic for attempts to exploit password weaknesses</td>
</tr>
</tbody>
</table>
## Technical solutions

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak file integrity checks</td>
<td>• Configure the operating system to only run signed code</td>
</tr>
<tr>
<td></td>
<td>• Test software and updates in a simulated environment prior to production deployment</td>
</tr>
<tr>
<td></td>
<td>• Obtain software/firmware directly from the vendor and not third-parties</td>
</tr>
<tr>
<td></td>
<td>• Work closely with vendor support to obtain file hashes and check hashes manually</td>
</tr>
<tr>
<td></td>
<td>• Monitor the network for firmware and logic updates</td>
</tr>
<tr>
<td>Vulnerable Windows operating systems</td>
<td>• Maintain an inventory of EOL operating systems</td>
</tr>
<tr>
<td></td>
<td>• Plan to upgrade or apply patches</td>
</tr>
<tr>
<td></td>
<td>• Deploy compensating controls for vulnerabilities</td>
</tr>
<tr>
<td>Undocumented third-party relationships</td>
<td>• Request or require that vendors validate patches for the third-party software to ensure interoperability.</td>
</tr>
</tbody>
</table>
Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. The information provided here is of a general nature and is not intended to address specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

© 2017 Baker Tilly Virchow Krause, LLP