WannaCry Response

FREQUENTLY ASKED QUESTIONS – JOHNSON CONTROLS MAY 2017

1. **I've heard about a significant cybersecurity attack on IT systems – what happened?**
   On Friday, May 12, a previously unknown strain of ransomware began affecting computer systems across the globe. Known as WannaCry or Wcry, the ransomware has caused significant disruptions at various types of organizations – banks, hospitals, telecommunications providers and other mission-critical organizations.

2. **What is ransomware?**
   Ransomware is an evolving type of malware (i.e. malicious code) that blocks access to sensitive files and/or electronic devices by automatically encrypting them upon infection. Ransomware also puts users at financial risk, because once files/devices are infected and files have been encrypted, access may be lost forever unless a ransom is paid or the virus removed and data restored from a known good back-up..

3. **What did Johnson Controls do when the company became aware of the WannaCry ransomware attack?**
   The first step was to activate the company's Product Security Incident Response Team (or PSIRT). The weekend of the attack, this team worked to evaluate and assess the impact of WannaCry on Johnson Controls building technology offerings, especially its flagship building automation system, *Metasys*®. An initial set of FAQs was developed to help account managers answer potential questions from customers and the company re-issued, via social media, existing guidance titled, "Ransomware and Your Building Automation System," as well as direct emails to our field. Customers were also helped to safeguard their information and properly update their systems.

4. **How does *WannaCry* work?**
   WannaCry affects computers running some older and unpatched versions of the Microsoft® Windows® operating systems. Initial reports indicate that this ransomware may first be introduced to a network by users clicking on a malicious link or opening an infected email attachment. Once introduced, the malware then spreads to other computers using a Windows Server Message Block (SMB) vulnerability. Files on affected computers are then encrypted for a ransom.

5. **Is the Johnson Controls *Metasys*® building automation system vulnerable to the WannaCry threat?**
   Computers running older or unpatched versions of the Windows operating system are potentially vulnerable to WannaCry. Certain models of *Metasys* network engines running older versions of *Metasys* software are potentially vulnerable. For more details, visit the Johnson Controls product security website.

6. **What can building owners and operators do to protect their *Metasys* building automation systems?**
   As a preventative measure, it is critical that building operators apply the patch that Microsoft released two months ago. There is information on how to implement the patch MS17-010 here. Even with the patch, building operators must protect their information and systems at all times. The best protection is to ensure your system is current with the latest *Metasys* software, and that your building automation system data and configuration files are routinely backed-up. If you would like more information on how to update or backup *Metasys*, please contact your local Johnson Controls representative.

7. **Why is it important to update to *Metasys* 8.1?**
   When building operators decide not to migrate their building automation system – just as with other electronic systems – they put their buildings at an increasing risk as malicious actors find new ways to exploit operating systems and IP connections. Johnson Controls updates and upgrades its building technology offerings, and – in the case of *Metasys* – we are in regular communication with Microsoft to prevent or eliminate any vulnerabilities that arise. *Metasys* 8.1 is able to help block the WannaCry virus from infiltrating the building automation system, because Johnson Controls has enabled an operational internal host firewall to block SMB network protocol port 445 (where WannaCry infiltrates).

8. **Is it possible for the *Metasys* 8.1 firewall to be disabled? Where can I go for additional help?**
   Yes. *Metasys* 8.1 has the firewall turned on by default, but operators may have chosen to disable the firewall, which will make the system vulnerable to WannaCry. If you have specific questions about best practices for *Metasys* or other Johnson Controls building technology products please contact your Johnson Controls local account manager or factory-trained technician. You may also email our Product Security Incident Response Team (PSIRT): beproductsecurity@jci.com.

9. **What else should I do to protect my information?**
   Regularly protect your software by implementing updates that come from Microsoft or other operating systems. Upgrading to the latest version of *Metasys* or other building automation system is always a best practice to safeguard building information and infrastructure. Be wary of suspicious emails, and do not click on unknown links or attachments. Never use your building automation system for general-purpose internet browsing. For more information on Johnson Controls product security, visit http://www.johnsoncontrols.com/productsecurity.

Johnson Controls