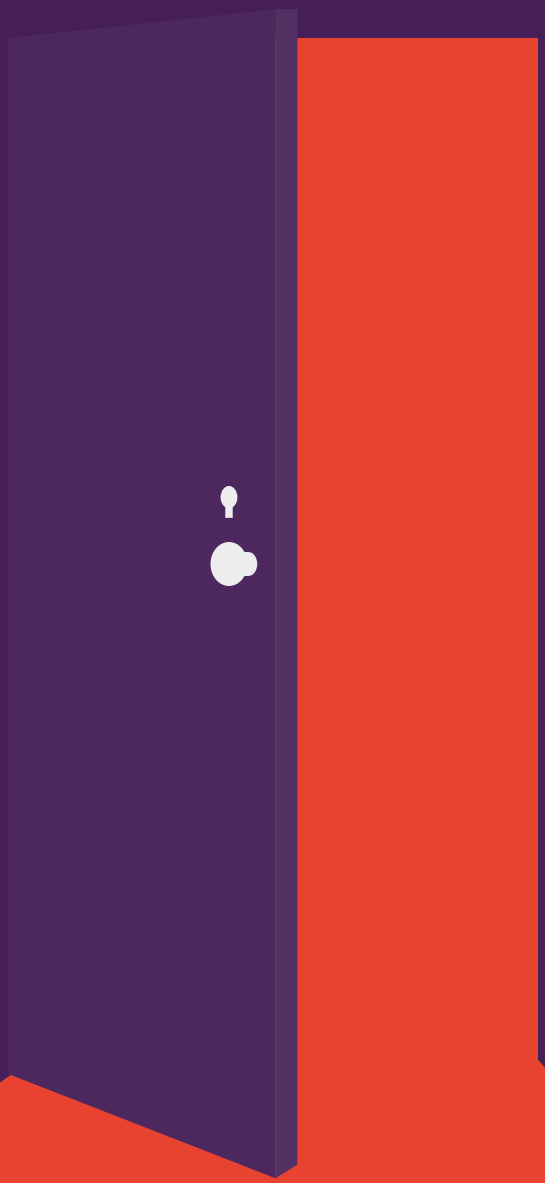
เอกสารข้อมูล

ช่องทางที่อาจเป็นอีกหนึ่งความเสี่ยง

งานวิจัยแสดงให้เห็นว่าเครื่องพิมพ์ตกอยู่ในความเสี่ยงที่จะถูกโจมตีทางไซเบอร์

ขณะที่ทีมไอทีให้ความสำคัญกับอุปกรณ์อื่นๆ ความปลอดภัยสำหรับเครื่องพิมพ์ถูกมองข้ามไป



เครื่องพิมพ์ตกเป็นเป้าได้ง่าย เพราะเครื่องพิมพ์ที่เชื่อมต่อกับเครือข่ายจำนวนมากไม่มีข้อจำกัดในการใช้งานและไม่ได้รับการล็อคอย่างปลอดภัย

แต่ภัยคุกคามเกิดขึ้นจริง และเป็นสิ่งที่ไม่ควรมองข้าม เครื่องพิมพ์ระดับองค์กรพัฒนาไปมากจนกลายเป็นอุปกรณ์ในเครือข่ายที่มีประสิทธิภาพ พร้อมกับมีช่องโหว่ต่างๆ เช่นเดียวกับอุปกรณ์อื่นๆในเครือข่าย จุดที่ไม่ปลอดภัยเหล่านี้ทำให้มีความเป็นไปได้ที่จะเกิดการโจมตีทางไซเบอร์ขึ้นอย่างมาก และยังเปิดโอกาสให้เข้าถึงข้อมูลทางการเงินและข้อมูลส่วนตัวของบริษัทคุณ อันจะก่อให้เกิดผลทางธุรกิจอย่างใหญ่หลวงตามมา

ระบุว่า 16% ของผู้ตอบคิดว่าเครื่องพิมพ์มีความเสี่ยงสูงต่อการคุกคาม/การละเมิดด้านความปลอดภัยซึ่งเป็นสัดส่วนที่น้อยกว่าเดสก์ท็อป/แล็ปท็อป และอุปกรณ์เคลื่อนที่อย่างมาก[1] และการรับรู้เช่นนี้ส่งผลต่อวิธีการจัดการความปลอดภัยเครือข่ายของพนักงานไอที ขณะที่องค์กรจำนวนเกือบสามในห้าแห่งมีการนำแนวปฏิบัติในการรักษาความปลอดภัยมาใช้กับเครื่องพิมพ์แต่อัตราส่วนเท่านี้ก็ยังถือว่าต่ำเมื่อเทียบกับอุปกรณ์อื่นๆ และทำให้เครื่องพิมพ์ตกอยู่ในความเสี่ยง เมื่อมีโซลูชันง่ายๆ ที่จะใช้ปกป้องจุดรับเข้านี้

เอกสารระเบียบมาตรฐานนี้จึงนำเสนอข้อมูลเกี่ยวกับความปลอดภัยของเครื่องพิมพ์ตามแบบสำรวจของ Spiceworks ผลกระทบจากการละเมิดความปลอดภัย และคุณสมบัติการรักษาความปลอดภัยในเครื่องพิมพ์ที่ทันสมัยซึ่งออกแบบมาเพื่อป้องกันการโจมตีทางไซเบอร์

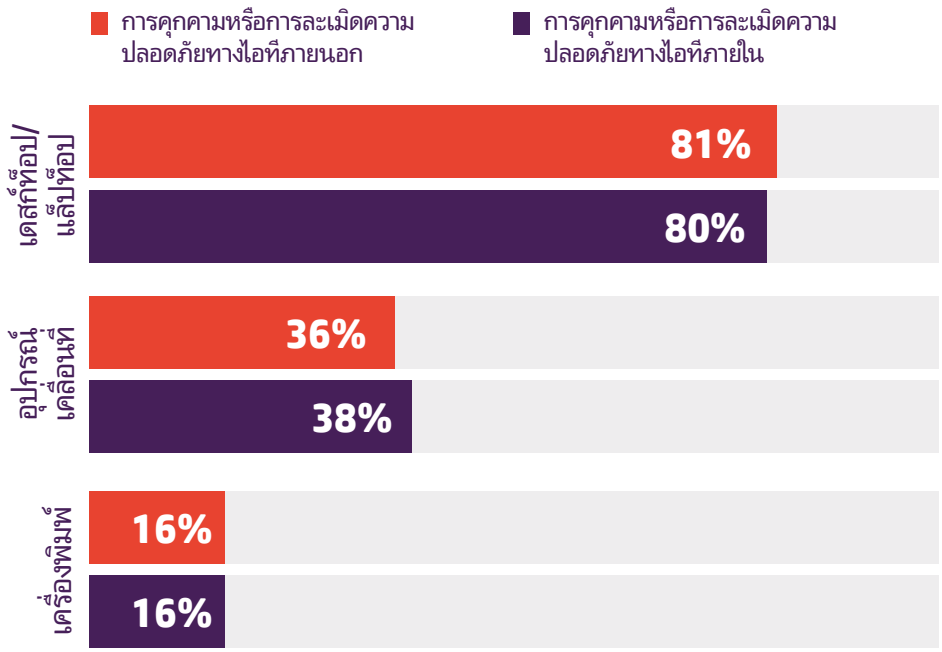
มีเพียง 16% ของผู้ตอบที่คิดว่าเครื่องพิมพ์มีความเสี่ยงสูงต่อการคุกคาม/การละเมิดด้านความปลอดภัย[1]

ช่องทางการโจมตี

ในแบบสำรวจของ Spiceworks 74% ของผู้ตอบ (สุทธิ) ระบุว่าองค์กรของตนเคยพบกับการคุกคามหรือการละเมิดความปลอดภัยทางไอทีจากภายนอกอย่างน้อยหนึ่งประเภทในปีที่ผ่านมา และ 70% (สุทธิ) เคยประสบกับการคุกคามหรือการละเมิดความปลอดภัยทางไอทีภายใน ซึ่งสาเหตุที่พบมากที่สุดมาจากความผิดพลาดของผู้ใช้งานการใช้อุปกรณ์ส่วนตัวเพื่อการทำงาน หรือการที่พนักงานใช้เครือข่ายที่บ้านหรือเครือข่ายสาธารณะเพื่อการทำงาน[1]

ภัยคุกคามหรือการละเมิดความปลอดภัยทางไอทีภายนอกที่พบมากที่สุด

ภัยคุกคามอันดับต้นๆ เล็ดรอดผ่านทางเดสก์ท็อปและแล็ปท็อปเป็นหลัก ขณะที่ภัยคุกคามอื่นๆ จะเข้ามาทางอุปกรณ์เคลื่อนที่และเครื่องพิมพ์[1] (สัดส่วน 16% ของภัยคุกคามที่มาทางเครื่องพิมพ์สูงขึ้นจาก 4% อย่างมาก ซึ่งเป็นตัวเลขที่พบในงานวิจัยที่คล้ายกันของ Spiceworksในปี 2014) นอกจากนี้ เป็นไปได้ว่าจำนวนการโจมตีผ่านทางเครื่องพิมพ์เป็นการคาดการณ์ที่ต่ำเกินไป เนื่องจากเครื่องพิมพ์ไม่ได้รับการตรวจสอบอย่างใกล้ชิดเท่ากับคอมพิวเตอร์และอุปกรณ์เคลื่อนที่



เรากำลังมองข้ามเครื่องพิมพ์ของเรา

ไม่ว่าในกรณีใด แบบสำรวจของ Spiceworks แสดงให้เห็นอย่างชัดเจนว่าการรักษาความปลอดภัยของเครื่องพิมพ์มักเป็นสิ่งที่นำมาพิจารณาภายหลัง

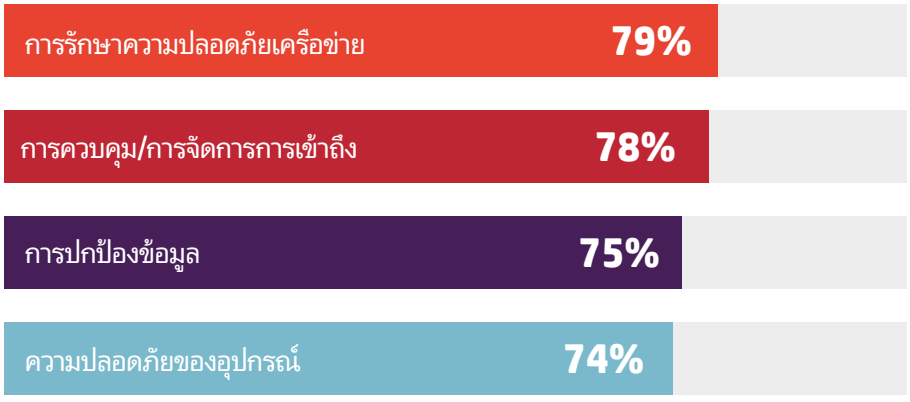
องค์กรต่างๆ ตระหนักถึงความสำคัญของเครือข่ายอุปกรณ์ และระบบรักษาความปลอดภัยข้อมูลเป็นอย่างดี อันที่จริง มากกว่าสามในสี่ของผู้ตอบแบบสำรวจใช้ระบบรักษาความปลอดภัยเครือข่าย การควบคุม/การจัดการการเข้าถึง การปกป้องข้อมูล หรือระบบรักษาความปลอดภัยอุปกรณ์ หรือทั้งหมดนี้รวมกัน[1]

แต่กลับนำโซลูชันเหล่านี้มาใช้กับเครื่องพิมพ์ไม่บ่อยครั้งมากนัก ขณะที่ 83% ของผู้ตอบใช้ระบบรักษาความปลอดภัยเครือข่ายสำหรับเดสก์ท็อป/แล็ปท็อป และ 55% ใช้สำหรับอุปกรณ์เคลื่อนที่ และมีเพียง 41% ที่ใช้ระบบนี้กับเครื่องพิมพ์[1]

และสำหรับระบบรักษาความปลอดภัยอุปกรณ์ความแตกต่างนี้ยิ่งเพิ่มมากขึ้น:

นอกจากนี้ จำนวนหนึ่งในสาม (28%) ของผู้ตอบไม่เคยกระทั่งใช้ใบรับรองความปลอดภัยสำหรับเครื่องพิมพ์ ซึ่งต่างจาก 79% ของผู้ตอบที่ใช้กับคอมพิวเตอร์ และ 54% ใช้กับอุปกรณ์เคลื่อนที่[1]

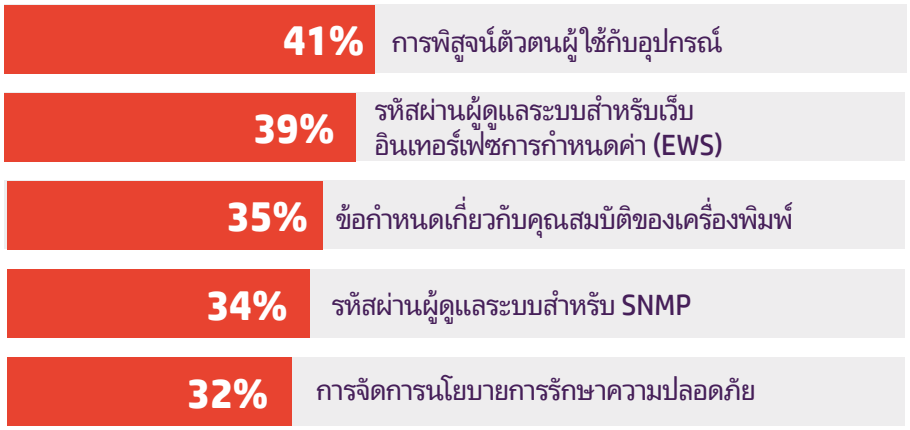
แนวปฏิบัติในการรักษาความปลอดภัยอุปกรณ์ที่ใช้กันมากที่สุด



ในบรรดาระบบป้องกันที่ใช้ในอุปกรณ์ทั่วไปมาตรการความปลอดภัยสำหรับเครื่องพิมพ์ที่ใช้กันมากที่สุดคือ การรักษาความปลอดภัยของเอกสารการรักษาความปลอดภัยเครือข่าย และการควบคุมการเข้าถึง แต่น้อยกว่าครึ่งหนึ่งของผู้ตอบแบบสอบถามกล่าวว่าองค์กรของพวกเขาใช้หนึ่งในมาตรการดังกล่าวกับเครื่องพิมพ์[1]

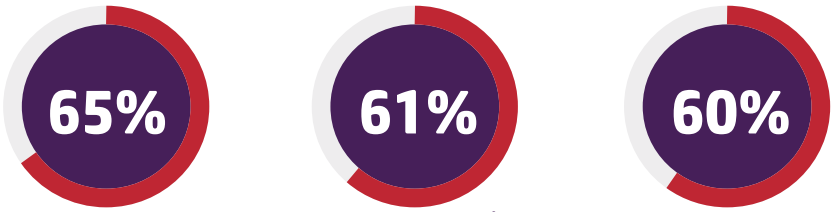
บางบริษัทมีแนวปฏิบัติในการรักษาความปลอดภัยสำหรับเครื่องพิมพ์โดยเฉพาะ แต่แม้กระนั้น แนวปฏิบัติก็มีความแตกต่างกันอย่างมาก องค์กรกว่า 40% ใช้การพิสูจน์ตัวตนผู้ใช้ และมีไม่ถึง 40% ที่ใช้รหัสผ่านผู้ดูแลระบบสำหรับอินเทอร์เฟซการกำหนดค่าเว็บ[1] ซึ่งสำหรับการป้องกันที่แข็งแกร่ง แต่ละองค์กรควรใช้วิธีการเหล่านี้ทั้งหมดผสมกัน และอื่นๆ อีกมากมาย

แนวปฏิบัติในการรักษาความปลอดภัยสำหรับเครื่องพิมพ์โดยเฉพาะที่ใช้กันมากที่สุด



เมื่อพูดถึงการปฏิบัติตามข้อกำหนดเกี่ยวกับอุปกรณ์และการปฏิบัติงานตรวจสอบภายใน ระบบควบคุมความปลอดภัยของเครื่องพิมพ์จะเกิดขึ้นช้ากว่าอุปกรณ์อื่นๆ เกือบทั้งหมด แม้ว่าเกือบ 90% ขององค์กรมีการนำนโยบายด้านความปลอดภัยข้อมูลมาใช้ แต่นโยบายเหล่านี้มักไม่ขยายครอบคลุมไปถึงเครื่องพิมพ์ด้วย ตัวอย่างเช่น แม้ว่า 57% ของผู้ตอบแบบสอบถามกล่าวว่าคอมพิวเตอร์ของตนมีการใช้ระบบป้องกันมัลแวร์ แต่มีเพียง 17% ที่นำไปใช้กับเครื่องพิมพ์[1]

เกือบ 9 ใน 10 ของผู้เชี่ยวชาญด้านไอทีกล่าวว่าองค์กรของตน
ใช้นโยบายด้านความปลอดภัยข้อมูลด้วยเหตุผลต่อไปนี้:



เพื่อให้ตรงตามกฎข้อบังคับ/มาตรฐานที่กำหนด

หลีกเลี่ยงความเสี่ยงที่จะเกิดขึ้น

กำหนดแนวปฏิบัติ/นโยบายด้านความเสี่ยง/การรักษาความปลอดภัยสำหรับผู้ใช้ปลายทาง

เป็นที่แน่ชัดว่าองค์กรไม่ได้ให้ความสำคัญกับการรักษาความปลอดภัยของเครื่องพิมพ์อย่างจริงจังมากเพียงพอ แต่อย่างที่เห็นว่านี่เป็นสิ่งที่เราควรให้ความสำคัญ

“เครื่องพิมพ์จำนวนมากยังคงมีรหัสผ่านตามค่าเริ่มต้นหรือกระทั่งไม่มีเลย หรือคนสิบคนยังใช้รหัสผ่านเดียวกัน” ไมเคิล โฮเวิร์ด หัวหน้าที่ปรึกษาด้านความปลอดภัยของ HP บอกกับ Computerworld เมื่อเดือนมิถุนายน “เครื่องพิมพ์ที่ไม่มีการป้องกันด้วยรหัสผ่านคือขุมทรัพย์สำหรับแฮกเกอร์ หนึ่งในการละเมิดที่เราพบได้บ่อยคือการโจมตีแบบคนกลาง (man-in-the-middle attack) ซึ่งแฮกเกอร์จะเข้าควบคุมเครื่องพิมพ์และเปลี่ยน [เอกสารที่เข้ามา] ไปยังแล็ปท็อปก่อนที่จะพิมพ์ออกมา แฮกเกอร์จึงสามารถเห็นทุกสิ่งที่ซีอีโอกำลังสั่งพิมพ์”[2]

ผลกระทบที่อาจเกิดขึ้นของการบุกรุกเครือข่าย

นักวิเคราะห์อาวุโสด้านภัยคุกคามทางออนไลน์โบกดาน โบเดอร์ชาทู จาก Bitdefender ให้ความเห็นว่าเครื่องพิมพ์มีช่องโหว่ด้านความปลอดภัยที่อาจเกิดขึ้นมากมาย “เราพบการตรวจสอบและส่งข้อมูลจำนวนมากในห้องปฏิบัติการประเมินช่องโหว่ของเรา เราเตอร์ไม่ใช่อุปกรณ์ที่อันตรายที่สุดบนอินเทอร์เน็ตอีกต่อไป แต่กลายเป็นเครื่องพิมพ์”[3]

ช่องโหว่นี้อาจส่งผลอย่างใหญ่หลวงต่อธุรกิจ เครื่องพิมพ์ที่ไม่ปลอดภัยเพียงเครื่องเดียวอาจทำให้อุปกรณ์ที่เชื่อมต่อกับทั้งเครือข่ายตกอยู่ในความเสี่ยงที่จะถูกโจมตี เปิดโอกาสให้แฮกเกอร์สามารถสอดแนมอุปกรณ์ที่อยู่ในเครือข่าย และเสี่ยงต่อความปลอดภัยของเครือข่ายทั้งหมด

1. การโทรติดต่อเจ้าหน้าที่เพื่อขอความช่วยเหลือและเวลาที่ใช้สนับสนุนเพิ่มขึ้น

2. ประสิทธิภาพ/ประสิทธิผลลดลง

3. เวลาดาวน์ไทม์ของระบบเพิ่มขึ้น

4. เวลาที่ใช้ในการติดต่อเพื่อขอรับความช่วยเหลือเพิ่มขึ้น

5. การบังคับใช้นโยบายสำหรับผู้ใช้ปลายทางเพิ่มขึ้น

เราได้เห็นผลลัพธ์ของการละเมิดความปลอดภัยทั้งหมดแล้วในแบบสำรวจของ Spiceworks ผู้ตอบกล่าวว่าผลกระทบห้าอันดับแรกของการละเมิดได้แก่:[1]

แต่การละเมิดความปลอดภัยของเครื่องพิมพ์อาจรุนแรงกว่านั้น โดยเฉพาะอย่างยิ่งหากคุณใช้เครื่องพิมพ์แบบมัลติฟังก์ชัน ซึ่งสามารถจัดเก็บข้อมูลที่พิมพ์ในรูปแบบ

อิเล็กทรอนิกส์ เพราะงานพิมพ์ซึ่งจัดเก็บไว้ในแคชของเครื่องพิมพ์ทำให้แฮกเกอร์สามารถเข้าถึงข้อมูลส่วนตัวหรือข้อมูลธุรกิจที่เป็นความลับได้

ที่น่ากังวลกว่านั้นคือ แฮกเกอร์สามารถเข้าถึงเครือข่ายบริษัทที่กว้างขึ้นผ่านเครื่องพิมพ์ที่ไม่ปลอดภัย และขโมยข้อมูลต่างๆ อาทิหมายเลขประกันสังคม ข้อมูลทางการเงินหรือบันทึกและเอกสารภายในได้ ซึ่งข้อมูลที่ถูกขโมยนี้ไม่เพียงส่งผลต่อพนักงานรายบุคคลเท่านั้น แต่ยังอาจถูกคู่แข่งนำไปใช้หรือก่อให้เกิดความเสียหายร้ายแรงต่อชื่อเสียงของบริษัท

โซลูชันง่ายๆ: คุณสมบัติด้านความปลอดภัยในตัว

แน่นอนว่าบริษัทจำเป็นต้องมีระบบรักษาความปลอดภัยแม้แต่กับเครื่องพิมพ์ ปัจจุบันเครื่องพิมพ์ระดับองค์กรที่ทันสมัยบางรุ่นมีคุณสมบัติด้านความปลอดภัยในตัวที่ใช้งานง่ายซึ่งช่วยปกป้องเครื่องพิมพ์จากภัยคุกคาม โดยคุณสมบัติเหล่านี้ได้แก่

- **การตรวจจับการโจมตี การป้องกัน และการซ่อมแซมอัตโนมัติ**
- **การใช้การติดตามเพื่อป้องกันการใช้โดยไม่ได้รับอนุญาต**
- **ตัวเลือกการลงชื่อเข้าใช้ที่ง่ายดาย เช่น PIN หรือสมาร์ทการ์ด**
- **เครื่องอ่านบัตร Proximity ที่ช่วยให้ผู้ใช้พิสูจน์ตัวตนได้อย่างรวดเร็ว และพิมพ์ข้อมูลได้อย่างปลอดภัยโดยใช้ป้ายชื่อพนักงาน**
- **การพิมพ์เอกสารสำคัญด้วยการเข้ารหัสอย่างปลอดภัย**

เมื่อคุณพิจารณาซื้อเครื่องพิมพ์เครื่องต่อไปไม่ว่าจะเป็นเครื่องพิมพ์ตั้งโต๊ะหรือเครื่องพิมพ์มัลติฟังก์ชัน ควรตรวจสอบคุณสมบัติการป้องกันความปลอดภัยในตัว และดูให้แน่ใจว่าได้เปิดใช้งานแล้ว ด้วยคุณสมบัติที่ใช้งานง่ายสำหรับเครื่องพิมพ์โดยเฉพาะไม่มีเหตุผลที่เครื่องพิมพ์จะตกอยู่ในความเสี่ยงอีกต่อไป นอกจากนี้ ด้วยเทคโนโลยี Internet of Things หรือ IoT แม้จะมีจุดเชื่อมต่ออื่นๆ อีกมากที่ต้องกังวล **แต่เครื่องพิมพ์ของคุณจะไม่เป็นหนึ่งในนั้นอย่างแน่นอน**

มองหาเครื่องพิมพ์ที่ปลอดภัยมากขึ้นอยู่หรือไม่
เรียนรู้เพิ่มเติม ›

แหล่งข้อมูล:

[1] Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC,on behalf of HP, November 2016

[2] "Printer Security: Is your company's data really safe?" *Computerworld*, 1 มิถุนายน 2016 http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things onthe Internet," *The Register*, 8 กันยายน 2016 http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/