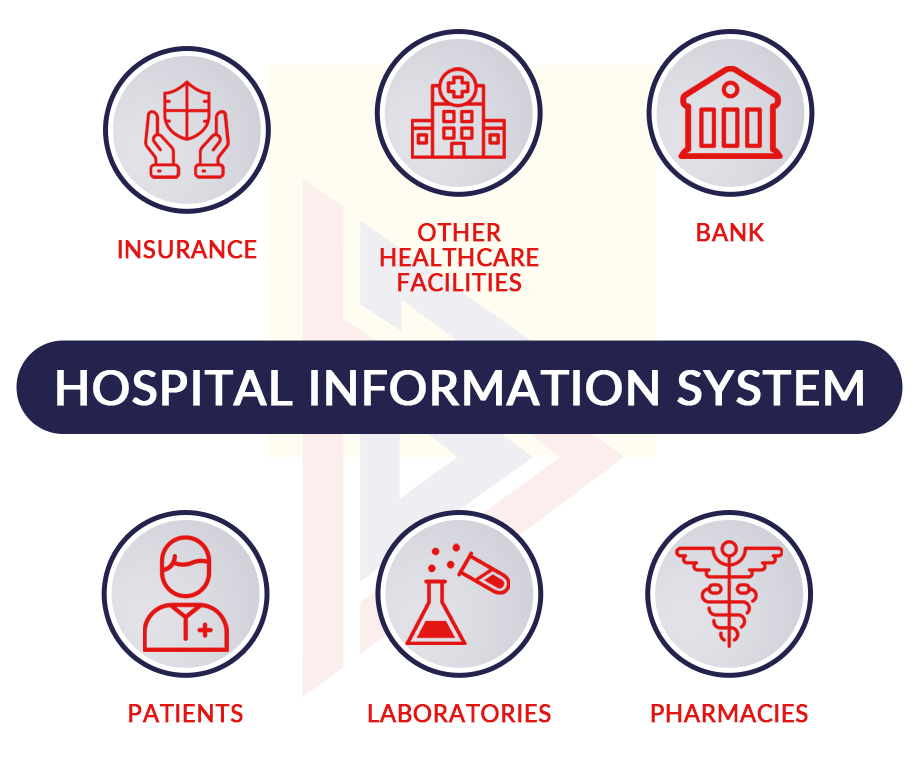
*Analyzing Obsolete Computer Systems in Healthcare*

Phanice Obasi   
*Computer, Information Sciences, and Data Sciences Department*  
*University of Wisconsin – River Falls*Wisconsin – United States  
phanice.obasi@my.uwrf.edu

line 5: phanice.obasi@my.uwrf.edu  
  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCID  
  
  
  
line 1: 4th Given Name Surname  
line 2: *dept. name of organization (of Affiliation)*  
line 3: *name of organization (of Affiliation)*line 4: City, Country  
line 5: email address or ORCI

# Introduction

Healthcare changes dramatically because of technological developments, from anesthetics and antibiotics to magnetic resonance imaging scanners and radiotherapy. Future technological innovation is going to keep transforming healthcare, yet while technologies (new drugs and treatments, new devices, new social media support for healthcare) will drive innovation, it is important to maintain a universal advancement in technology to reduce the chances of some sectors being left behind to use age-old systems. As indicated below, hospital systems ensure seamless collaboration and flow of data between the healthcare institution and insurance companies, other healthcare facilities, the bank, patients, laboratories, and pharmacies. Having universally advanced technology systems is crucial to improve care coordination, population health management, and improved patient education.



1. Key collaborators for hospital information systems

In the following sections, I will explore how obsolete systems are still integrated in the healthcare industry today, why that is the case, and what effects this brings about to healthcare institutions.

# Emergence obsolete systems

According to a 2020 study released by Palo Alto Networks- a security consulting company, a significant portion of Internet-connected imaging devices in hospitals run outdated operating systems. The company found that 83% of these devices run on outdated software that cannot be updated even if the software contains known vulnerabilities that hackers can exploit. This number has increased significantly compared to 2018, which is in line with Microsoft’s end of support for Windows 7 earlier this year. Many computers run even older operating systems, including Windows XP, and Microsoft dropped support for Windows XP in 2014. Imaging equipment includes X-rays, MRI, mammograms and CAT scans, all of which require computers to provide support and control. Security experts say keeping the operating system updated is one of the most important steps to keep hackers away from the device, and when institutions stop updating their machines, the system becomes obsolete over time.

The research conducted by Palo Alto was meant to identify the top IoT threats and provide recommendations that organizations can take to immediately reduce IoT risk in their environments. The following is a chart showing the extent to which medical imaging devices are running on unsupported operating systems:

.

Chart

Description automatically generated with medium confidence

1. Breakdown of OS support for medical imaging devices

Most notably, the chart reveals that 83% of medical imaging devices are running on unsupported operating systems. This reflects a 56% jump from 2018 due to the Windows 7 operating system reaching its end of life, leaving hospital organizations vulnerable to attacks that can disrupt care or expose sensitive medical information.

# Vulnerabilities of obsolete systems

In the example of operating systems shown above, when updates stop being released, hackers don’t stop looking for exploitable vulnerabilities. When a hacker eventually finds a vulnerability that can destroy an outdated operating system, manufacturers sometimes still provide updates, but there is no guarantee that they will. This leaves healthcare organizations at the brink of attack.

The main vulnerability of obsolete systems is that they’re susceptible to attacks from hackers. The aftermath of the attacks (what hackers choose to do after successfully infiltrating an institution’s network), varies. Hackers may have multiple motivations to target equipment in hospitals. Among them, imaging and other medical equipment, such as infusion pumps and patient monitoring systems, may be vulnerable to ransomware attacks. Hackers can use the computing power of hospital computers to mine cryptocurrencies, an attack known as “crypto hijacking.” This may cause the device to overheat or malfunction.

Hackers may choose to lock the system and require payment for the hospital staff to regain control. The bulk of attacks targeting the healthcare sector are ransom Trojans. Using this method, attackers aim to shut down certain operations, before then demanding a ransom to reverse the disruption. Unlike most other industries, disruptions in healthcare can put human lives and health at risk, and criminals know this. Considering the severity of this threat, and the fact that healthcare providers are unable to sustain operational downtimes, it is no surprise that some would feel obligated to pay the ransom. However, this is strongly discouraged as there is no guarantee that attackers would stand down and not repeat the threat at a later date.

Other attacks that target patients themselves are just as, if not more, devastating. The Vastaamo attack, for example, shocked the industry and everyone involved. Over one weekend in October 2020, thousands of patients inundated victim support services having received emails demanding €200 in bitcoin to prevent contents of their sessions with therapists being made public. This appalling act against vulnerable individuals shows the extent to which criminals will go for financial gain.

In addition, another motivation is the access to the large amount of data that healthcare institutions hold. This data varies from patient and practitioner personal information, financial information related to patients and other institutions, and medical test results. Physicians and computer scientists at the University of California San Diego have shown that medical test results can be easily modified remotely by attacking the connections between hospital laboratory devices and medical record systems. The researchers also suggest that these unsecured medical record systems and unsecured medical devices could be putting patient lives at risk, and high-profile targets like heads of state and celebrities could be more at risk than the general public. demonstrated the attack, known Pestilence, at the Black Hat 2018 conference in Las Vegas on Aug. 9. While the vulnerabilities of unsecured networks are not new, the researchers showed how the vulnerabilities could be exploited to compromise patient health. The vulnerabilities come from the standards that are used to transfer patient data within hospital networks, known as Health Level Seven (HL7) standards. HL7 was created in the 1970s as a way for devices and systems in a medical facility to communicate. Surprisingly, the system has since been untouched by cybersecurity advances that have been made in the last 40 years. Currently, patient data is being circulated in an unsecured way because of HL7 standards being implemented on aging medical equipment by personnel who have little to no cybersecurity training. The main concern is that the data is being transmitted in unencrypted and plain text though networks that do not need passwords and other forms of authentication. There have already been a few cybersecurity threats to hospital networks over the last few years and given the manipulation of critical healthcare infrastructure has the potential to directly impact human life, protecting data from being manipulated remains an important task for all stakeholders in the healthcare industry.

## Emerging Trends

All devices connected to the Internet are known as Internet of Things (IoT). In the research done by Palo Alto, the following are emerging trends that all industries, but more specifically healthcare, should be aware of:

* **98% of all IoT device traffic is unencrypted,** exposing personal and confidential data on the network and allowing attackers the ability to listen to unencrypted network traffic, collect personal or confidential information, then exploit that data for profit on the dark web.
* **51% of threats for healthcare organizations involve imaging devices**, disrupting the quality of care and allowing attackers to exfiltrate patient data stored on these devices.
* **72% of healthcare VLANs** (Virtual Local Area Networks) **mix IoT and IT assets**, allowing malware to spread from users’ computers to vulnerable IoT devices on the same network.

## Top IoT Threats

Threats continue to evolve to target IoT devices using new sophisticated and evasive techniques, such as peer-to-peer command and control communications and worm-like features for self-propagation. Coupled with a weak device and network security posture, attackers have ample opportunity to compromise IoT systems. To further break this down:

* **57% of IoT devices are vulnerable to medium- or high-severity attacks,** making IoT the low-hanging fruit for attackers.
* **41% of attacks exploit device vulnerabilities**, as IT-borne attacks scan through network-connected devices in an attempt to exploit known weaknesses.

The Covid-19 pandemic also brought to light some significant defects in the healthcare systems. For example, there have been several ransom Trojan attacks during the pandemic, including Ryuk, orchestrated by the Russia-based Wizard Spider advanced persistent threat (APT) group. Dozens of hospitals and healthcare institutions have been impacted by Ryuk during the pandemic, where COVID-19 has pushed hospitals and healthcare organizations and staff to their limits.

Given that the vulnerabilities in the IoT devices used in healthcare institutions makes them easy targets, they are most often used as a steppingstone for lateral movement to attack other systems on the network. The research also found that password-related attacks continue to be prevalent on IoT devices due to weak manufacturer-set passwords and poor password security practices. More advanced threats include running botnets to conduct DDoS attacks via IoT devices and malware spreading across the network via worm-like features, enabling attackers to run malicious code to conduct a large variety of new attacks. The following is a breakdown of the top IoT threats:

Chart

Description automatically generated

1. Breakdown of the top IoT threats

## Steps to Reduce IoT Exposure

Technology is used more and more in our daily lives, and it’s so deeply infiltrated into the industries we interact with every day. With such a significant increase in adoption that shows no signs of slowing down, organizations need to be prepared with a strong IoT security strategy. There are a myriad of ways enterprises are being left vulnerable to security threats, which can easily lead to some very dire circumstances if exploited. To reduce IoT threats, you, as an institution should:

1. Assess assets

Perform routine assessments of network devices, systems and software platforms, monitor for suspicious activity and identify solutions that minimize risk. Getting a solid understanding of your network and all the devices on it can enable you to conduct a risk assessment to identify cyber threats and vulnerabilities within your environment, then tailor solutions like firewalls, encryption and authentication solutions to fit your needs.

1. Patch printers and other easily patchable devices

For devices that need system upgrades, it is important to make sure that this is done as soon as possible, to ensure that the institutions are using the latest and most secure systems. The patches are meant to fix bugs and vulnerabilities that are found on earlier versions of that software.

1. Perform an information assessment

Identify the data your institution holds, how you use the data, how you protect the data and who has access. Healthcare institutions typically hold an overwhelming volume of valuable and sensitive data in both electronic and paper format, including personal, financial, and medical data on current, former, and prospective patients, staff and vendors. Once you inventory the types of data your organization has and the purpose for holding the data, you can then identify departments and resources that deal with data privacy issues and create a data protection plan that meets your institution’s unique needs.

1. Prepare a cybersecurity incident response plan

There’s so much at stake in the event of a cyberattack. Data security breaches can shut down your institution, cost thousands of dollars in ransom fees and cause unmeasurable reputational damage. Develop a plan that alerts the right person in your institution to contact in the event of a breach, figure out how to remediate systems to stop the incident and decide more generally how you’ll respond to a cyberattack. Create a plan proactively that’s tailored to your specific needs and address preparation, detection and analysis, containment, eradication, and recovery.

1. Revisit insurance policies

U.S. institutions can take out cyber insurance policies to cover some of the risks that come with data breaches. If you are considering such a policy, pay special attention to exceptions that may not cover all cyber risk. If you have a policy, make sure it updates to cover evolving risks.

1. Consider hiring a CISO

Chief information security officers can contribute expertise and skills on information security issues and be in charge of reviewing and commenting on internal policies and procedures, assessing data management policies and practices, and researching and recommending technologies for mitigating security risks. You can hire a part-time CISO or go as far as hiring a full-time CISO.

1. Review vendor relationships

Healthcare institutions typically share information with service providers for a number of reasons, including processing and booking appointments, processing insurance claims and cash payments or to store patient data, for instance. While most services providers are running on up-to-date systems, some are not. Do your due diligence and vet vendors before granting access to personal information. Insist that service providers sign a written contract to protect confidential patient and institutional data.

# Are institutions aware of these risks?

It is possible that key stakeholders in these healthcare organizations are aware that their technology systems need to be updated every now and then. However, given the sheer workload that these institutions have (ie. Taking care of patients, making sure they’re receiving payments from insurance companies, keeping track of their staff, and basically having to maintain normal day to day hospital routines), it is easy to overlook the need for an upgrade simply because “the machine is still running just fine”. The significant risks of having obsolete systems are overlooked, and the weight of the matter only comes to light once the institution is under attack.

In fact, not many people actually think that your local hospital down the road can be the subject of a cybersecurity attack. When people first think about the most common victims of cyber-attacks, their minds automatically shift to the big money targets, like banks and retail. Yet, one other victimized industry suffers numerous attacks, with the potential to cause devastating and even traumatic consequences - the healthcare sector. Whilst not the most lucrative target in terms of immediate financial gain, the healthcare sector holds stores upon stores of sensitive medical data which can be used in attacks to commit fraud, or as perfect leverage for blackmail.

Incidents such as the **Vastaamo Psychotherapy Centre breach** (an incident where mental health startup built its business on easy-to-use technology, patients came in and told their therapists confidential information, but all that sensitive information was leaked after a data breach) demonstrate the severe impact an attack can have on individuals. And it doesn’t stop there. Criminals will use any weakness, large or small, to their advantage – COVID-19 being the most recent. Last year, more than one in four UK cyber-attacks were related to COVID-19, and the attack on the COVID vaccine supply chain is just one example.

# Why institutions have not yet upgraded to updated systems, and possible ways to get them there

The healthcare industry has missed two technology change cycles, so many organizations are burdened with a lot of legacy healthcare IT infrastructure. Bob Renner, CEO of cloud-based data management firm Liaison Technologies, says that information technology needs to be “ripped and replaced” every 10 years, but healthcare has missed two of those cycles, so it is “ripe and ready to upgrade and update.”

Because healthcare has gone for so long without really modernizing their infrastructure, it becomes more difficult to do it over time. The following is a run-down of some of those problems:

1. For one thing, cloud computing wasn’t widely available back then; Everything was behind a firewall. Data was secured physically, and it was localized in data centers and monolithic applications. Now, as everything is moving to the cloud, healthcare organizations are facing a pretty big challenge logistically, technically, and from a resource standpoint, to update their infrastructure.
2. When healthcare organizations begin to upgrade their technology, they need to consider the data integration problem. Some healthcare CIOs are opting for one centralized platform (this involved holding all data and institutional functionalities in one place), such as Centricity, Epic, or Cerner. While this solves the data integration problem, it comes with “significant tradeoffs” in terms of functionality.
3. When healthcare organizations deploy new technology, they will need to hire “top talent” to implement that technology. Unfortunately, it's already a tight labor market, and if you want to upscale your entire IT staff, that's a big financial commitment that not many institutions can take up.
4. Lastly, there’s a recent trend where graduates of good computer science and engineering programs do not want to enter healthcare because of the legacy technology. It's a vicious cycle where if you have legacy technology, you're not going to attract top talent, and once you don't have the top talent, you can't make the conversion to modern technology. Recognizing this talent shortage, many healthcare organizations are focusing on staff retention efforts in addition to hiring new staff, rather than upgrading their technology.

Ultimately, to get healthcare institutions to upgrade their systems, healthcare CIOs should try to make the business case for upgrading infrastructure by focusing on cost savings. They can argue that new technology will lower the costs of claims processing, for example. That is a difficult case to make when you are talking about a major digital transformation, because you actually need to inject some finances into upgrading the systems, before you can actually see the overall effect of the system upgrade down the line. The CIOs are the people with the visions in these institutions and they should try to push these visions as much as possible; when trying to make a shift to a data-centric environment, you have to have a certain amount of vision and belief that your data's going to be valuable, and it's going to allow your company to innovate, transform the patient experience and improve patient care in the long run.

Upgrading IT infrastructure will provide a competitive advantage for healthcare organizations over those who still have legacy technology. Patients have a lot of information at their fingertips, so they can research to find the best healthcare provider with the best technology in their area. As organizations consider upgrading their legacy IT infrastructure, they should approach it in a strategic way: The first decision that these health systems or hospital systems need to make is, do they want to be best of breed where they can adopt new applications as they come available fairly quickly or do they want to get locked into a single vendor solution and live with the tradeoffs. Whoever's running IT or making the decision really needs to make that strategic decision first, and that's going to dictate if the upgrade is going to be a big project or if it's going to be a series of smaller projects. Most importantly, the system upgrade will be to the benefit of the patients that the healthcare institution serves, and to the institution itself.

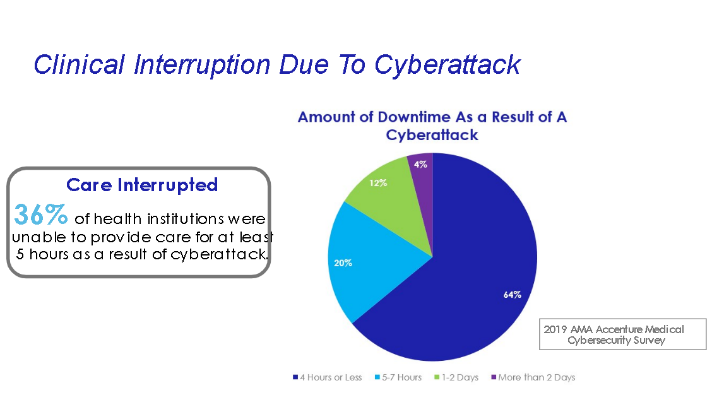
# Healthcare institutions that are most at risk

Cybercriminals have targeted hospitals with growing frequency in recent years, identifying the millions of recently digitized patient files as a treasure trove of unguarded information. Hospitals have historically been vulnerable to security breaches due to their reliance on expensive, aging medical equipment, their inability to halt patient care to perform time-consuming software updates, and a workflow that depends on the constant input and accessing of data on different devices. Those complications, combined with the high black-market value of medical records, makes such facilities prime targets for a growing number of sophisticated criminals.

Breaches at hospitals, insurance companies and other health care-related businesses have been climbing in California in recent years, with 30 incidents reported in 2015, up from eight in 2009, according to the U.S. Department of Health and Human Services. Nationally, about 1,500 data breaches have been reported in health-care settings since 2009. Last year, the Ponemon Institute, a privacy and security research group, found that about half of health organizations are attacked by hackers one or more times in any given 12-month period.

In short, all sectors in healthcare are at risk, and those include but are not limited to: Hospitals, Health insurance companies, Clinical Laboratories, Pharmacies, Clinics and medical offices, Nursing homes, Mental health and addiction treatment centers, Imaging and radiology centers, Dialysis facilities, Orthopedic rehabilitation centers, Hospice centers, Dental institutions, Telehealth institutions, and Blood banks.

In one report, 36% of health institutions were unable to provide care for at least 5 hours as a result of cyberattack. The following chart shows a breakdown of the downtime some institutions have faced as a result of being attacked:



1. Breakdown of institutional downtime due to cyberattacks

# Consequences of holding onto these obsolete systems

## Financial Costs

The average cost of a healthcare data breach is £5.27 million, which is one of the most expensive data breaches across all sectors. These costs include remediation following the attack, getting services back online and putting in place measures to prevent a similar attack happening again. In addition to this, organizations may need to pay large fines to regulators if they have failed to implement the required level of security. The GDPR has a maximum fine of £18 million, or four percent of income, whichever is greater. For medical institutions, these figures are enormous and could leave them on the brink of collapse. For example, a large healthcare organization may lose up to US$23.3 million as a result of cyber-attacks. The figure below shows that breakdown.

A picture containing diagram

Description automatically generated

1. Economic cost of cyber attacks on a large healthcare organization

## Decreased staff productivity

A new study, “*The Economic and Productivity Impact of IT Security on Healthcare*”, found that the use of pagers and other outdated communication technologies decreases clinician productivity and increases patient discharge times; thus, costing U.S. hospitals an unnecessary abundance of $8.3 billion annually. This survey also revealed that doctors, nurses, and other caregivers waste more than 45 minutes per day as a result of outdated communication technologies still used in many healthcare organizations today. This is not only costing the average U.S. hospital nearly $1 million annually but is also costing the average hospital more than $550,000 per year in lost revenue. The solution to these outstanding costs is modernizing the technology within hospitals, which maximizes face time with patients, and by providing quality care effectively, this gives patients positive experiences at the heath facilities.

## Putting lives at risk

There have been a few cybersecurity threats to hospital networks over the last few years and the data that is compromised could be manipulated to put patients’ lives at risk. First, a lot of personal information is stored in hospitals: financial information can be stolen, and patients’ credit cards may be maxed out, and their bank accounts drained, physical, and mailing addresses could make people subject to burglaries and murder attempts, and medical data could show attackers how to potentially end someone’s life. Attackers could infiltrate medical laboratory testing devices, computers, and servers to gain access to medical records. Doing so will allow the attacking team to run tests like blood and urine analysis while intercepting the results to change them and send the changed information back to a medical records system. One of the tests that can be changed is a normal blood test. The results could be changed to show that a patient was suffering from diabetes, which would cause a physician to prescribe an insulin drip. An insulin drip in a patient who doesn’t need it could lead to a coma or death. Attackers could also change a normal blood test to show that a patient had extremely low potassium, which a doctor would prescribe a potassium IV that would cause heart attack in a healthy patient.

The fact that lives are at risk makes it extremely crucial that medical record systems and medical devices should be password-protected and secured with a firewall. Many medical devices are still running on Windows XP operating systems, which is no longer supported by Microsoft, which means vulnerabilities go unfixed. Such systems should be upgraded. The hospital IT staff should be trained on cybersecurity issues and trained to enable defenses against potential attacks. Cybersecurity should also be part of the FDA approval process for healthcare devices and manufacturers would benefit from using the newest and most secure operating systems to ensure the proper cybersecurity needs.

##### Acknowledgment

I would like to express my gratitude to my primary supervisor, Professor Jacob Hendricks, who guided me throughout this project. I would also like to thank my CIDS 484 classmates who offered deep insight into the.

##### REFERENCES

1. Hypponen, Mikko. “How Outdated Medical Systems Leave Patient Records at Risk.” Healthcare Digital, 11 Sept. 2021, https://healthcare-digital.com/technology-and-ai/how-outdated-medical-systems-leave-patient-records-risk.
2. “2020 Unit 42 IOT Threat Report 2020 Unit 42 IOT Threat Report.” Palo Alto Networks, 3 Nov. 2020, https://unit42.paloaltonetworks.com/iot-threat-report-2020/.
3. Caiola, Sammy. “Decades-Old Specialized Equipment Makes Hospital a Prime Target for Hackers.” GovTech, GovTech, 23 Apr. 2021, https://www.govtech.com/health/decades-old-specialized-equipment-makes-hospital-a-prime-target-for-hackers.html.
4. Donovan, Fred. “Outdated Healthcare IT Infrastructure Can Weigh down Organizations.” HITInfrastructure, 26 Nov. 2018, https://hitinfrastructure.com/news/outdated-healthcare-it-infrastructure-can-weigh-down-organizations.
5. Gaudet, Kate. “Healthcare Loses $8.3 Billion per Year Due to Outdated Technology.” Imprivata, 12 July 2013, https://www.imprivata.com/blog/healthcare-loses-83-billion-year-due-outdated-technology.
6. Kirsh, Danielle, and William K. “How Outdated Medical Record Systems and Devices Could Risk Lives.” Medical Design and Outsourcing, 26 Sept. 2018, https://www.medicaldesignandoutsourcing.com/outdated-medical-record-systems-devices-risk-lives/.
7. “Outdated Software Still Run in 83% of U.S. Healthcare Systems.” LIFARS, a SecurityScorecard Company, 27 Mar. 2020, https://lifars.com/2020/03/outdated-software-still-run-in-83-of-u-s-healthcare-systems/.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published**